



# شبکه‌های کامپیوتری

مهندس مهدی رجبی

مدرس دانشگاه جامع علمی و کاربردی



## ✓ شبکه چیست؟

اساساً یک شبکه کامپیوتری شامل حداقل دو کامپیوتر است که از طریق یک کانال ارتباطی به منظور به اشتراک گذاری منابع به هم وصل شده‌اند.

## ✓ Network یا شبکه‌افزار

علمی است که فرآیندها، قوانین، تجهیزات و کلیه امور مربوط به برقراری یک شبکه را مورد بررسی قرار می‌دهد.

## ✓ منابع شبکه

منابع فیزیکی که قابل مشاهده هستند مانند چاپگر

منابع منطقی که قابل مشاهده نیستند مانند بانک‌های اطلاعاتی، نرم‌افزارهای تحت شبکه

## ✓ نیازمندی‌های شبکه

در شبکه علاوه بر موارد فوق نیازمندی‌هایی به منظور برقراری ارتباط لازم است. که این نیازمندی‌ها شامل موارد زیر است:

- ✓ کامپیوتر (PC) که البته امروزه تبلت‌ها و گوشی‌های هوشمند نیز جزء این دسته محسوب می‌شوند.
- ✓ رسانه انتقال (Media) که شامل نوع رسانه‌ای که وظیفه اتصال سیستم‌ها را برعهده دارد که می‌تواند کابل مسی، امواج وایرلس و یا فیبرنوری باشد.
- ✓ کارت شبکه (NIC) هم می‌تواند از نوع وایرلس یا کابلی باشد.
- ✓ سیستم‌عامل تحت شبکه (Domain) که زمانی مورد استفاده قرار می‌گیرد که ما قصد راه‌اندازی یک دامین در سطح شبکه به منظور مدیریت متمرکز را داشته باشیم که در قسمت‌های آینده اشاره خواهیم کرد.

## ✓ دلایل استفاده از شبکه

استفاده از ساختار شبکه اهدافی دارد که این اهداف، ما را در بهبود شرایط یاری می‌کند. نمونه‌ای از این اهداف و دلایل استفاده از شبکه را در زیر مشاهده می‌کنید:

- حذف محدودیت‌های جغرافیایی:

شما با استفاده از شبکه می‌توانید محدودیت‌های مکانی و جغرافیایی را پشت سر بگذارید. مثالی از این بخش استفاده از پست الکترونیکی است. زمانی که شما از پست الکترونیکی استفاده می‌کنید، فارغ از مکان جغرافیایی وی می‌توانید به صورت آنی پیامی را برای وی ارسال کرده و او نیز آن را تحویل گرفته و مطالعه کند.

- صرفه جویی در زمان و هزینه:

به طور مثال شما می‌توانید از سیستم‌های تلفن اینترنتی مانند viber و یا امثال آن است که امکان تماس رایگان از طریق اینترنت را برای شما امکان پذیر می‌کند. در این حالت فقط شما هزینه اتصال به اینترنت را می‌پردازید.

- به اشتراک گذاشتن منابع:

به اشتراک گذاشتن اطلاعات در وب یا وبلاگ ها، امکان اشتراک گذاری پرینترها در شبکه و مواردی از این دست مثالی برای این بخش است.

- امنیت:

شاید این بخش کمی تامل بر انگیز باشد، چرا که در برخی موارد شنیده ایم که شبکه امن نیست. حال چرا یکی از مزایای استفاده از شبکه امنیت است؟

شما می توانید با راه اندازی یک دامین، دسترسی های مربوط به کاربران را تعیین و محدود نمایید و یا می توانید پورت های USB سیستم های کاربران را غیر فعال نمایید. با انجام چنین مواردی، شما قادر خواهید بود تا از آلوده شدن سیستم ها به ویروس تا حدی جلوگیری کنید که این خود گامی به سوی امنیت است. موارد دیگری هم وجود دارد که به آن اشاره خواهیم کرد.

### ✓ مواردی که در طراحی یک شبکه باید مد نظر قرار گیرد.

اندازه سازمان مورد نظر باید مشخص شود تا در طراحی اولیه با اطلاعات کافی بتوان به نحو احسن شبکه را راه اندازی نمود.

سطح امنیتی که برای شرکت یا سازمان در نظر گرفته می شود هم حائز اهمیت است.

نوع فعالیت سازمان به منظور طراحی و پیاده سازی هر چه بهتر ساختار شبکه باید در نظر گرفته شود.

مقدار ترافیک نکته دیگری است که برای عدم بروز مشکلات پهنای باند و بروز اختلال در شبکه باید به آن پرداخت.

میزان بودجه دارای درجه اهمیت بالایی در طراحی شبکه می باشد. زیرا شما با میزان بودجه مشخص به طور مثال آیا می توانید از سویچ های سیسکو در شبکه استفاده کنید یا باید به سویچ های معمولی غیر قابل مدیریت اکتفا کرد.

### ✓ شبکه ها معمولاً به دو قسمت تقسیم می شوند:

۱- انواع شبکه از لحاظ منطقی

۲- انواع شبکه از لحاظ فیزیکی

- انواع شبکه از لحاظ منطقی

### ✓ شبکه های نظیر به نظیر peer to peer

این مدل برای شبکه ای با کمتر از ۱۰ کامپیوتر پیشنهاد می گردد که در آن ایستگاه ویژه ای جهت نگهداری و اشتراک منابع وجود ندارد. نکته ای که در این مورد حائز اهمیت است، این امر می باشد که ممکن است شما ۳ کامپیوتر را هم به صورت دامین پیاده سازی کنید. تمام سه موردی که در این بخش به آن اشاره می شود، بستگی به سیاست های سازمان و شرکت مربوطه دارد. نام دیگر این ساختار Work Group هم می باشد.

## ✓ شبکه های مبتنی بر سرویس دهنده server based

در این مدل یک کامپیوتر به عنوان سرویس دهنده تمام فایل های اشتراکی، بانک های اطلاعاتی و ... را نگهداری کرده و هر کاربر می تواند از طریق اتصال به آن فایل ها را به روی سیستم خود منتقل کند. در واقع پردازش در سمت سرویس دهنده صورت می گیرد. ساختار شبکه های بانکی در قدیم و حتی برخی در حال حاضر از این نوع ساختار استفاده می کنند.

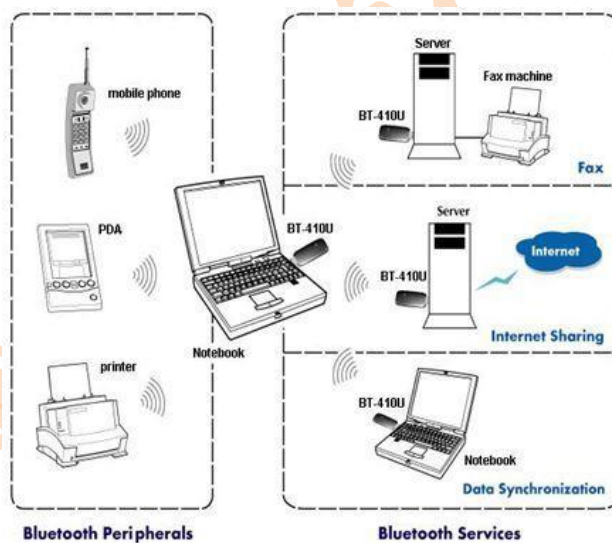
## ✓ شبکه های مبتنی بر سرویس دهنده / سرویس گیرنده client/server

در این مدل یک ایستگاه درخواست انجام کارش را به سرویس دهنده ارائه کرده و سرویس دهنده پس از اجرای وظیفه محوله نتایج را به ایستگاه درخواست کننده عودت می دهد. در این مدل حجم اطلاعات مبادله شده در مقایسه با مدل دوم کمتر بوده و کاربرد بالاتری دارد. نام دیگر این ساختار شبکه های Domain می باشد. استفاده از دایرکتوری سرویس هایی مانند Active Directory در این نوع ساختارها رایج است.

## • انواع شبکه از لحاظ مقیاس

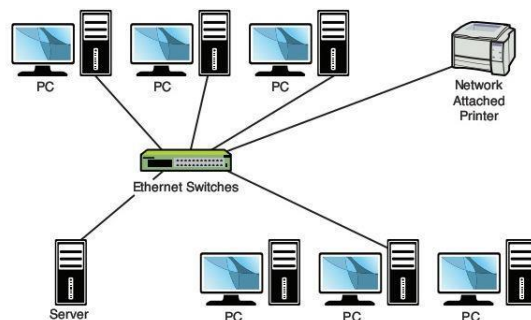
## ✓ Pan ( Personal Area Network )

شبکه شخصی یک شبکه کامپیوتری است که برای ارتباطات میان وسایل جانبی که اطراف یک فرد می باشند مانند تلفن ها، رایانه های جیبی، پرینتر و .... بکار می رود.



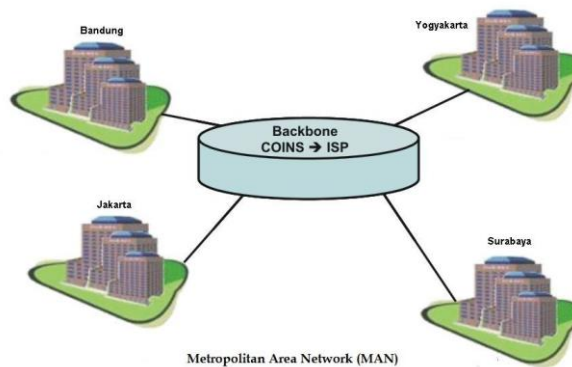
## LAN ( Local Area Network ) ✓

شبکه محلی یک شبکه کامپیوتری است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمانها را پوشش می دهد.



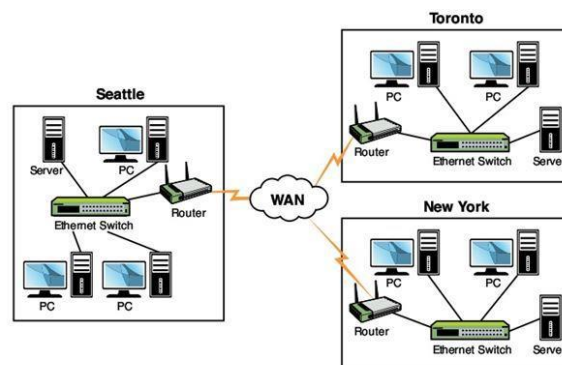
## Man (Metropolitan Area Network ) ✓

شبکه کلان شهری یک شبکه کامپیوتری بزرگ است که معمولاً در سطح یک شهر گسترده می شود. در این شبکه ها معمولاً از زیرساخت بی سیم و یا اتصالات فیبر نوری جهت ارتباط محل های مختلف استفاده می شود.



## Wan ( Wide Area Network ) ✓

شبکه گسترده یک شبکه کامپیوتری است که نسبتاً ناحیه جغرافیایی وسیعی را پوشش می دهد (از یک کشور به کشوری دیگر یا از یک قاره به قاره ای دیگر). این شبکه ها معمولاً از امکانات انتقال خدمات دهندگان عمومی مانند شرکت های مخابرات استفاده می کند.



## ✓ توپولوژی (Topology)

توپولوژی شبکه تشریح کننده نحوه اتصال فیزیکی کامپیوترها در یک شبکه به یکدیگر است.

• انواع توپولوژی:

خطی (BUS)

ستاره (STAR)

حلقه ای (RING)

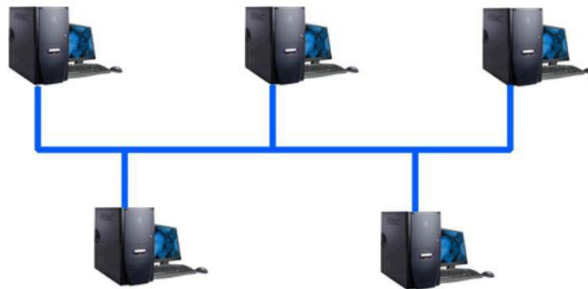
درختی (TREE)

اتصال کامل یا توری شکل (MESH)

وایرلس (Wlan)

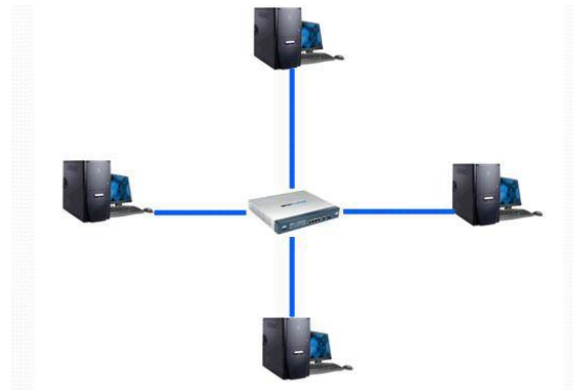
## ✓ توپولوژی خطی (BUS):

در شبکه ای که از توپولوژی باس استفاده می شود، همه کامپیوترها پشت سر همدیگر و در یک خط، توسط کابل شبکه به یکدیگر متصل شده اند. برای توپولوژی باس از کابل های کواکسیال استفاده می شود که امروزه دیگر به ندرت به چشم می خورند. مشکل اصلی توپولوژی باس این است که یک مشکل کوچک در یک کانکتور، ترمیناتور یا کابل شبکه، کل شبکه را تحت تاثیر قرار می دهد. علاوه بر این وقتی مشکلی در نقطه ای از شبکه به وجود آید، کل شبکه به دو سگمنت یا قطعه تقسیم می شود و هر یک از آن بخش ها بدون ترمیناتور خواهند شد و در نتیجه هیچ یک از دو بخش شبکه قادر به برقراری ارتباط و تبادل داده ها نمی باشند. امروزه از شبکه های باس به ندرت استفاده می شود. در این نوع شبکه وقتی کامپیوتری شروع به ارسال داده می نماید، جریان وارد کابل شده و در هر دوسو حرکت می کند و به تمام کامپیوترها می رسد ولی تنها در کامپیوتر مقصد قابل استفاده است. وقتی جریان به انتهای کابل رسید برگشت پیدا می کند و با جریان داخل سیم تداخل پیدا می کند برای جلوگیری از این مطلب در دوسر شبکه از ترمینال استفاده می شود.



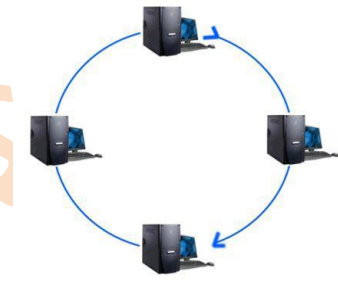
## ✓ توپولوژی ستاره ای (STAR):

در این توپولوژی از یک وسیله مرکزی برای کابل کشی استفاده می شود که هاب یا تمرکزدهنده نامیده می شود. در یک شبکه ستاره ای هر یک از کامپیوترها توسط یک کابل مجزا به هاب متصل می شوند. LAN های ستاره ای می توانند از چندین نوع کابل متفاوت، که شامل کابل های فیبر نوری و زوج ماریچ می شوند، استفاده کنند. هاب هر سیگنال را که دریافت می کند روی تمام پورت های خود پخش می کند و بدین صورت سیگنالی که یک کامپیوتر می فرستد، توسط تمام کامپیوترهای دیگر موجود روی LAN دریافت می شود. تحمل خطا در چنین شبکه هایی بالاتر است و اگر یک کابل یا کانکتور دچار مشکل شود، فقط کامپیوتری که با آن کابل یا کانکتور به هاب متصل است تحت تاثیر قرار می گیرد. اگر هاب دچار اشکال شود، کل شبکه مختل می شود.



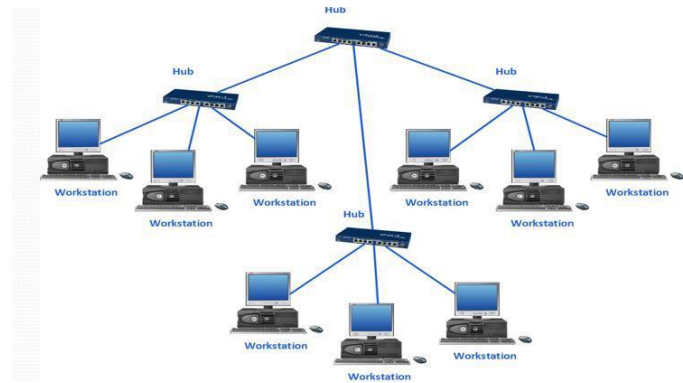
### ✓ توپولوژی حلقه‌ای (RING):

در این نوع شبکه‌ها به جای اینکه دو انتهای کابل شبکه بسته شود کامپیوترها به همدیگر متصل می‌شوند و یک حلقه را تشکیل می‌دهند. در این نوع شبکه داده از کامپیوتری ارسال می‌شود و در حلقه ایجاد شده به کامپیوترهای دیگر می‌رسد و هر سیستم که داده برای وی است، آن را برداشته و در غیر این صورت داده را به سیستم بعدی خواهد داد. اگر سیگنال ارسالی یک کامپیوتر بعد از گذر از تمام کامپیوترهای دیگر به کامپیوتر تولید کننده برسد بدون اینکه در سیستمی دریافت شود، اصطلاحاً گفته می‌شود سیگنال مرده (Drop) است. در برخی شبکه‌های حلقوی از نوع خاصی از هاب به نام MAU که اطلاعات را از یک پورت دریافت می‌کند و به نوبت به تک تک پورت‌های دیگر می‌فرستد استفاده می‌شود. در شبکه‌های مبتنی بر MAU وقتی کامپیوتری بسته‌ای ارسال می‌کند MAU آن را دریافت و یکی یکی به کامپیوترهای شبکه می‌فرستد تا مقصد بسته، آن را تحویل بگیرد.



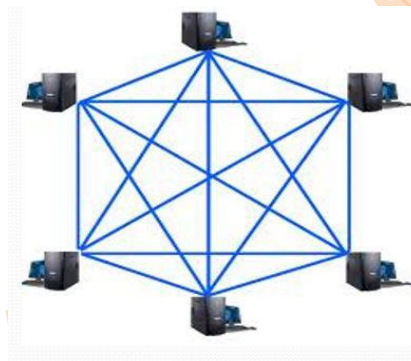
### ✓ توپولوژی درختی (TREE):

ممکن است تصور کرده باشید که شبکه‌ای که از توپولوژی ستاره‌ای استفاده می‌کند محدود به تعداد پورت‌های هاب خود می‌باشد. اما در صورتی که قرار باشد شبکه گسترش پیدا کند، بعد از اشغال تمام پورت‌های هاب، این امکان وجود دارد که یک هاب و یا حتی در بعضی موارد دو یا سه هاب دیگر به شبکه اضافه کنید. برای اینکار هاب دوم باید با استفاده از یک کابل استاندارد و پورت خاصی که به این منظور روی هاب‌ها تعبیه شده‌است و پورت uplink نام دارد، به هاب دوم متصل شود.



### ✓ توپولوژی توری شکل (MESH):

در یک شبکه مش هر کامپیوتر یک اتصال مستقیم و اختصاصی به هر یک از کامپیوترهای دیگر شبکه دارد. مزیت یک شبکه مش، تحمل خطای بالای آن می باشد. چون هیچ مشکل یگانه ای وجود ندارد که روی بیش از یک کامپیوتر تاثیر بگذارد از چنین توپولوژی در شبکه های تجاری بزرگ استفاده می شود چون شبکه را قادر می سازد در مقابل اختلالات ممکن از قبیل مشکلات احتمالی در مسیریاب، هاب و کابل ها، در حد امکان مصون شوند.



### ✓ توپولوژی (WLAN):

در این توپولوژی برای ارتباط بین کامپیوترها به جای کابل از فناوری وایرلس (Wireless) استفاده می شود. هر کامپیوتر دارای یک کارت شبکه بدون سیم می باشد و با کامپیوتر دیگر اگر در محدوده آن باشد می تواند اطلاعات مبادله کند.

Ad-hoc در نوع دیگر پیکربندی این توپولوژی با استفاده از سخت افزاری به نام Access Point ایجاد می شود که با استفاده از این سخت افزار می توان تبادل اطلاعات را مدیریت نمود. با استفاده از Access Point می توان یک شبکه LAN را با یک شبکه WLAN متصل نمود.

مزایا استفاده در مکان هایی که امکان کابل کشی وجود ندارد برقراری ارتباط در حال حرکت گسترش بدون نیاز به سیم کشی از لحاظ اقتصادی مقرون به صرفه است نسبت به شبکه های کابلی هزینه راه اندازی بیشتری دارد.



## فصل دوم

# Network Cabling

### ✓ مدهای ارتباطی

این مدها تعیین کننده روش مبادله داده و تعیین کننده جهت ارسال و دریافت داده بین دو وسیله می باشد.

#### • انواع مدهای ارتباطی مبادله

✓ یک طرفه (Simple Mode): در این نوع مبادله، فقط یک طرف قادر به ارسال داده می باشد و طرف دیگر فقط دریافت کننده بوده و قادر به ارسال داده نمی باشد. بدین صورت مبادله به صورت یک طرفه صورت می پذیرد. فرستنده رادیو و تلویزیون نمونه ای از این ارتباط می باشند.

✓ مبادله دوطرفه غیرهمزمان (Half Duplex Mode): در این روش هر دو طرف قادر به ارسال و دریافت داده می باشند، ولی به صورت همزمان این کار انجام نمی گیرد. مانند دستگاه بی سیم مبادله

✓ دوطرفه همزمان (Full Duplex Mode): در این روش دو طرف هم قادر به ارسال اطلاعات و هم قادر به دریافت آن می باشند از دستگاهی که از این قابلیت استفاده می کند، می توان به تلفن اشاره نمود.

### ✓ پهنای باند (Bandwidth)

به تفاوت میان بالاترین و پایین ترین فرکانس هایی که یک سیستم ارتباطی قادر به ارسال آن می باشد، گفته می شود.

#### • Noise

عامل مخربی است که شکل سیگنال ها را تغییر می دهد و باعث اختلال در انتقال اطلاعات می گردد.

#### انواع Noise

۱- حرارتی

۲- (القای الکتریکی توسط موتورهای مکانیکی مثل موتور ماشین)

۳- هم شنوایی (اثر میدان مغناطیسی یک کابل بر کابل مجاور خود مثل اثر کابل های فشار قوی برق)

## ✓ انواع کابل ها

## کابل Coaxial

کابل های کوآکسیال یا هم محور جزء اولین کابل هایی بودند که در زمینه انتقال اطلاعات بکار گرفته شدند این کابل از دو هادی داخل یکدیگر تشکیل شده است که با یک پوشش پالستیکی همانند شکل از هم جدا شده اند.



از کانکتورهای BNC برای اتصال این نوع کابل ها به کامپیوتر استفاده می گردد.



از این کابل ها در توپولوژی BUS استفاده می گردد.

✓ انواع کابل کوآکسیال از نظر ضخامت:

Coaxial Thin Net ضخامت این کابل ۳۳/۱ اینچ بوده و حداکثر برد آن ۰.۸۳ متر است.

Thick Net ضخامت این کابل ۳/۱ اینچ بوده و حداکثر برد آن ۳۱۱ متر است.

انواع کابل Coaxial از نظر نوع روکش:

PVC: ارزان قیمت بوده و با سوختن، گاز سمی تولید می کند و برای کابل کشی خارج از ساختمان استفاده می شود.

plenum grade: گرانتر از کابل های PVC بوده و با سوختن گاز سمی تولید نمی کند و برای کابل کشی داخل ساختمان استفاده می گردد.

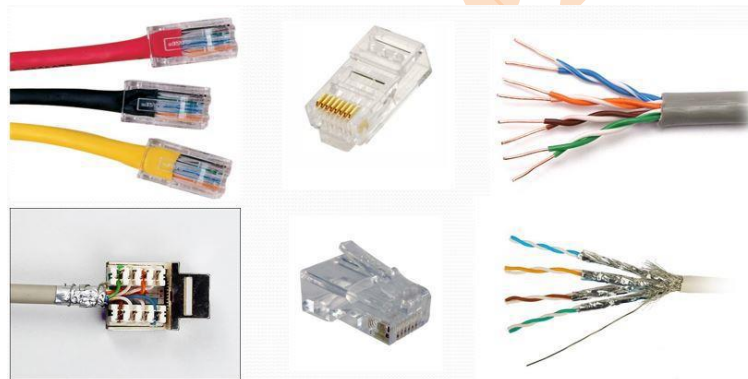
کابل زوج به هم تابیده Twisted pair: این نوع کابل شامل ۸ رشته سیمی بوده که دو به دو به هم پیچیده هستند که چهار تای آن برای ارسال اطلاعات و چهار تای آن برای دریافت اطلاعات است و در آن از کانکتورهای RJ۲۳ استفاده می گردد.

✓ انواع کابل زوج به هم تابیده Twisted pair UTP :

بدون محافظ (UTP)unshielded twisted pair: استفاده از این نوع کابل ها در شبکه های محلی متداول تر از نوع STP می باشد. این نوع از کابل ها بدون محافظ بوده و در برابر انواع نویز آسیب پذیر می باشند.

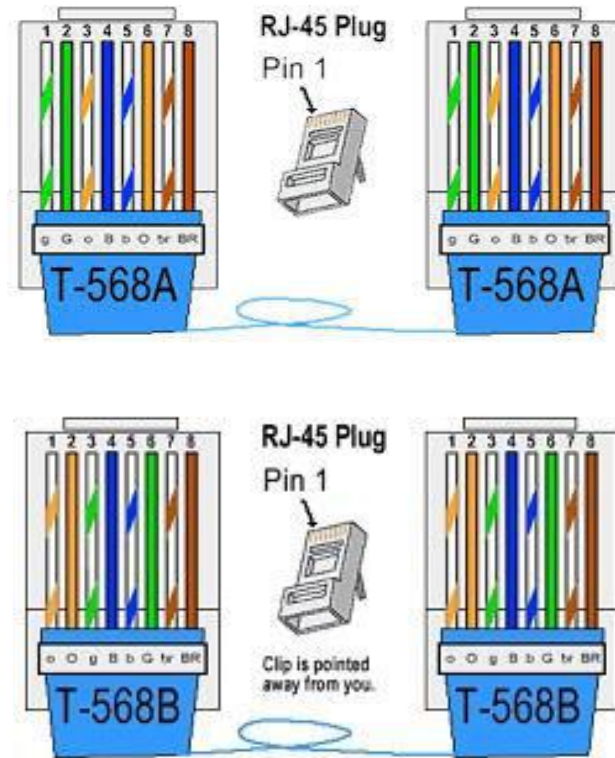
محافظدار (STP)shielded twisted pair: این کابل های نسبت به نوع قبل انعطاف کمتری داشته و به علت مقاومت در برابر امواج الکترومغناطیسی از این نوع کابل ها در شرایط خاص استفاده می شود.

کاربرد	Type
فقط صوت ( کابل های تلفن )	Cat ۱
داده با سرعت ۴ مگابیت در ثانیه	Cat ۲
داده با سرعت ۱۰ مگابیت در ثانیه	Cat ۳
داده با سرعت ۲۰ مگابیت در ثانیه	Cat ۴
داده با سرعت ۱۰۰ مگابیت در ثانیه	Cat ۵

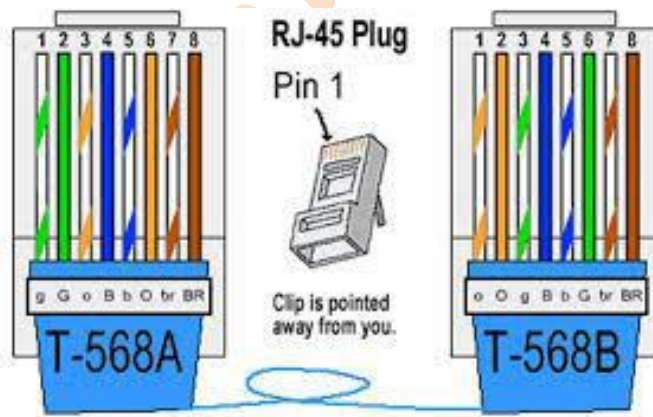


### ❖ کابل کشی

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت، ظرافت خاص و پایبندی به اصول کابل کشی ساخت یافته، انجام شود. در هنگام سوکت زنی و تهیه کابل شبکه نوع رنگ بندی کابل شبکه و چینش رشته های کابل از اهمیت زیادی برخوردار است. در ساختار چینش رشته های کابل دو استاندارد فراگیر وجود دارد که به استاندارد A و B معروف است. رنگ بندی در استاندارد A و B را در شکل زیر مشاهده می نمایید.



حال اگر شما در دو سر کابل از استاندارد A و یا از استاندارد B استفاده نمایید، به کابل تولید شده اصطلاحاً مستقیم یا Straight گفته می‌شود و زمانی که یک طرف کابل را استاندارد A و طرف دیگر را استاندارد B قرار دهید، به کابل تولید شده اصطلاحاً Cross گفته می‌شود.



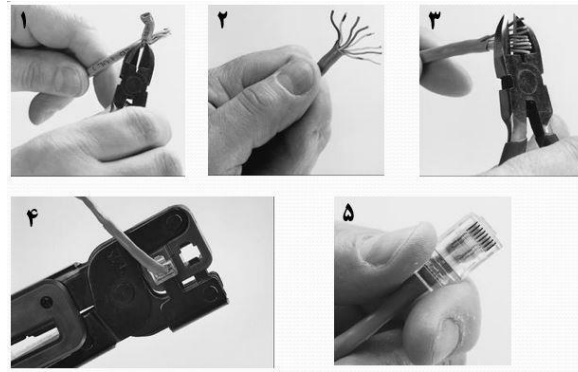
#### ✓ موارد استفاده کابل‌های Cross و Straight:

در مواقعی که می‌خواهیم دو دستگاه یکسان را به یکدیگر متصل نماییم از کابل Cross استفاده می‌کنیم. مانند اتصال دو کامپیوتر یا دو روتر به یکدیگر، که در این حالت از کابل Cross برای اتصال استفاده می‌شود. البته استثنائاتی هم در این مورد وجود دارد، مانند اتصال کامپیوتر به روتر که در این مورد نیز از کابل Cross استفاده می‌گردد.

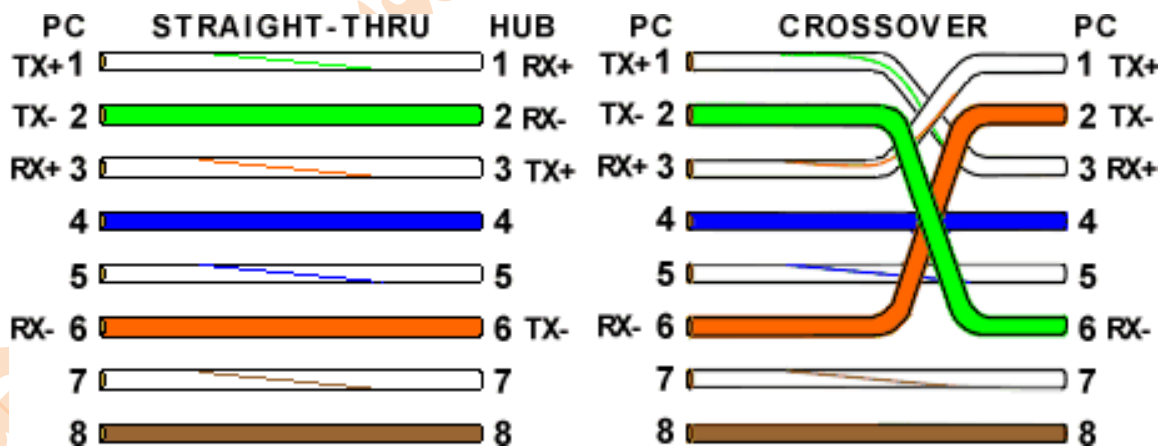
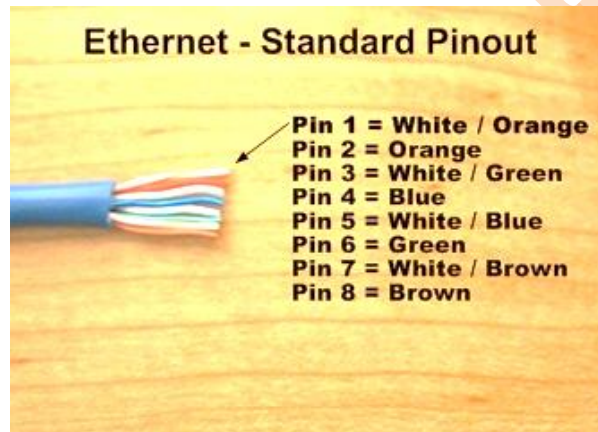
در اتصال کامپیوتر به سویچ یا هاب و اتصال کامپیوتر به مودم و غیره از کابل Straight استفاده می‌شود. لازم به ذکر است که استفاده از این دو نوع کابل به منظور تفاوت ساختار دستگاه‌ها در ارسال و دریافت می‌باشد که اکثر دستگاه‌های امروزی قادر به تبدیل سیگنال‌های دریافتی و ارسالی بوده و با هر دو نوع از کابل‌ها کار خواهند کرد.

برای ایجاد کابل های UTP از تجهیزات زیر استفاده می گردد:

آچار کانکتور - سیم چین - سوکت - کابل



ساخت کابل شبکه کراس و مستقیم cross & Straight Ethernet cables



## ✓ فیبر نوری Fiber Optic

از کابل های دیگر متفاوت بوده و به جای انتقال سیگنال های الکترونیکی در داخل سیم، پالس هایی از نور را در میان پلاستیک یا شیشه انتقال می دهد. در این نوع کابل ها از کانکتورهای SC و ST استفاده می گردد.

## ✓ مزایای استفاده از فیبر نوری

در برابر امواج الکترومغناطیسی مقاوم هستند اندازه آن کوچک و دارای پهنای باند بسیار وسیع در حد گیگاهرتز می باشد قابلیت انتقال اطلاعات در مسافت های طولانی حدود ۱۲۰ کیلومتر، تنها عیب این نوع کابل در هزینه نصب و نگهداری آن می باشد.



## • انواع فیبر نوری Fiber Optic

فیبر نوری از لحاظ زاویه شکست نور و انعکاس آن کار کرده به طوری که انعکاس آن بستگی به قطر کابل دارد که انواع آن به دو دسته زیر تقسیم بندی می شود.

✓ single mode fiber (SMF): از این نوع کابل که تک مد نیز نامیده می شود به منظور انتقال اطلاعات در فواصل طولانی استفاده می گردد. در این نوع فیبر نوری از یک لیزر (ILD) inject laser diode به عنوان منبع نوری استفاده می گردد.

✓ multi mode fiber (MMF): از این نوع کابل که چند مد نیز نامیده می شود برای انتقال اطلاعات در فواصل کوتاه استفاده می گردد و در آن از (LED) light emitting diode به عنوان منبع نوری استفاده می گردد.

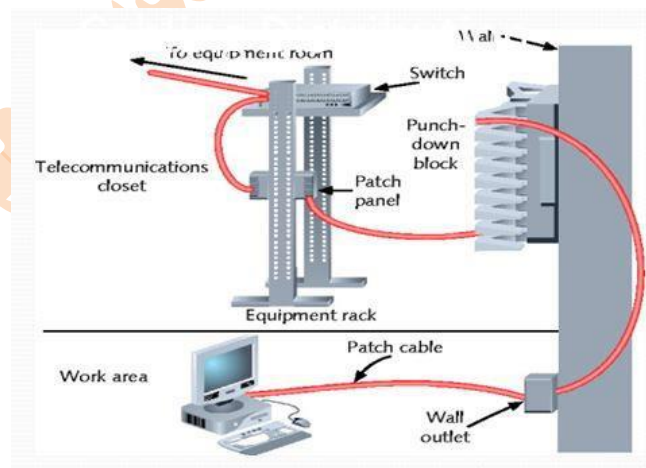
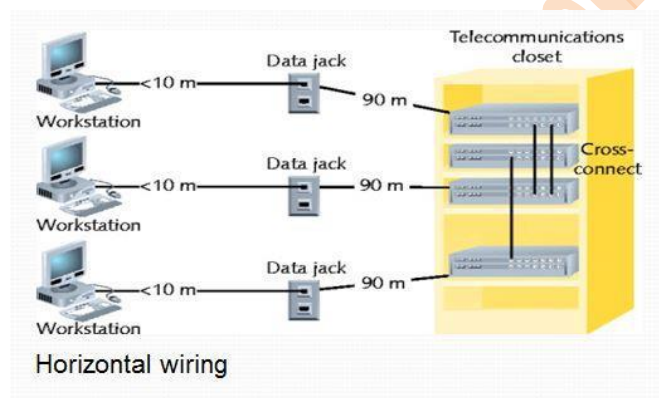
## • Patch Panel

برای ارتباط از سیستم کلاینت تا سویچ در یک ساختار شبکه، باید کابل کشی انجام شود. معمولاً این کابل از داخل داکت در اتاق کلاینت تا اتاق سرور که سویچ داخل آن می باشد، عبور می کند. داکت وسیله ای برای مرتب نمودن کابل ها است که معمولاً از جنس پلاستیک خاص بوده و دارای مقسم به منظور جدا کردن کابل های برق از شبکه است و می تواند برق را نیز در کنار کابل شبکه انتقال دهد. نمونه ای از داکت را در تصویر زیر، پایین تصویر Patch Panel مشاهده می کنید.





در یک شبکه معمولاً یک کابل مستقیماً از کلاینت به سویچ متصل نمی‌شود. ابتدا یک کابل کوچک از سیستم کلاینت به داکت درون اتاق وی متصل می‌شود که این کار از طریق نصب Face Plate مطابق شکل بالا روی داکت صورت می‌گیرد. در مسیر داکت یک کابل تا اتاق سرور کشیده می‌شود. در اتاق سرور سر دیگر کابل به یک Patch Panel متصل می‌شود. پس از اتصال به آن، یک کابل کوچک از Patch Panel به سویچ متصل می‌شود. به شکل‌های زیر دقت کنید.



در تصویر زیر نیز شما سرعت و محدودیت های سرعت در شبکه های کابلی یا Ethernet را مشاهده می کنید.

Ethernet Types	Bandwidth Capacities
Standard Ethernet	10 Mbps: 10 million bits per second (that is 10 megabits per second)
FastEthernet	100 Mbps: 100 million bits per second (that is 100 megabits per second)
Gigabit Ethernet	1 Gbps: 1 billion bits per second (that is 1 gigabits per second)
10-Gigabit Ethernet	10 Gbps: 10 billion bits per second (that is 10 gigabits per second)
100-Gigabit Ethernet	100 Gbps: 100 billion bits per second (that is 100 gigabits per second)

### ❖ مخابرات بی سیم

یکی از انواع راه های ارسال اطلاعات، ارسال به وسیله امواج مایکروویو و بدون سیم است.

### انواع مخابرات بدون سیم

در این روش انتقال اطلاعات بین ایستگاه ها از طریق امواج مایکروویو صورت می گیرد که انواع آن به شکل زیر است:

✓ **مخابرات زمینی:** برای این منظور از آنتن های بشقابی شده و در جاهایی که امکان کابل کشی وجود ندارد مورد بهره برداری قرار می گیرد.

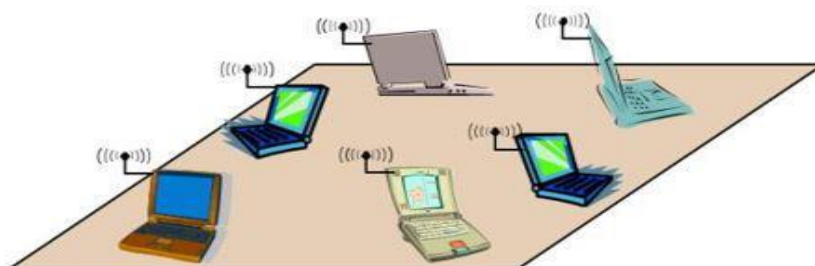
✓ **مخابرات ماهواره ای:** در این روش انتقال اطلاعات توسط ماهواره هایی که حول زمین هستند بین دو ایستگاه زمینی صورت می گیرد و در مواقعی که مخابرات زمینی امکان پذیر نباشد مورد استفاده قرار می گیرد.

### روش های دیگر مخابرات بی سیم

- WiFi
- Wimax
- Bluetooth

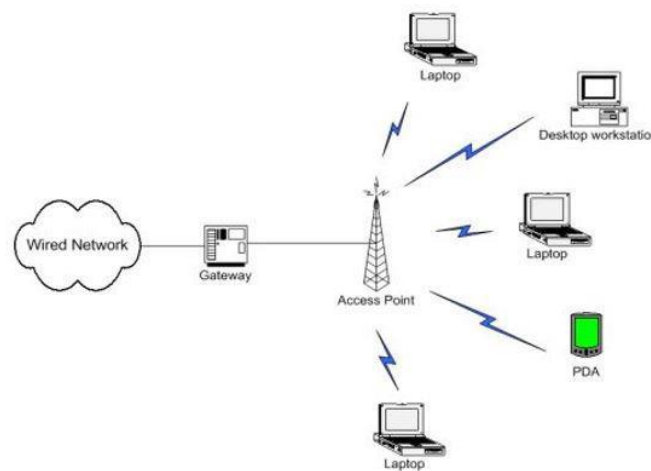
در شبکه های بی سیم دو ساختار برای نحوه اتصال کلاینت ها در نظر گرفته می شود که شامل Ad-hoc و Infrastructure می باشد.

Ad-hoc: شبکه هایی که در ساختار آن از Access Point استفاده نشده و سیستم ها با یکدیگر ارتباط برقرار می کنند. از این نوع شبکه زمانی که فاصله کمی بین کامپیوترها وجود دارد مورد استفاده قرار می گیرد.





Infrastructure: در این ساختار از یک Access Point استفاده می‌شود. سیستم‌ها ابتدا باید به AP متصل شده و سپس با یکدیگر ارتباط برقرار نمایند. منطقه تحت پوشش در این ساختار بیشتر از شبکه‌های Ad-hoc می‌باشد.



#### • اصطلاحات رایج در شبکه‌های وایرلس

**Service Set Identifier (SSID):** در واقع شناسه و نام Access Point است که وجه اشتراک بین AP و تمام کلاینت‌هایی است که قصد اتصال به آن را دارند. این نام به صورت پیش فرض اسم شرکت سازنده می‌باشد که باید آن را تعویض نمود.

**Chanel:** معمولاً بین یک تا چهارده کانال در هر AP وجود دارد. این چهارده کانال حداقل بین بیشتر فرکانس تا کمترین فرکانس است. اگر دو AP در یک کانال فعالیت کنند، افت سرعت در آن‌ها بوجود خواهد آمد. معمولاً پیشنهاد می‌شود برای کارایی بهتر AP خود در کانالی قرار دهید که AP دیگری وجود نداشته باشد.

از نرم‌افزار **WiFi Analyzer** برای این منظور استفاده می‌گردد که در تصویر زیر نمایی از این نرم‌افزار که در سیستم عامل اندروید استفاده شده‌است را مشاهده می‌نمایید.



BSSID: آدرس فیزیکی Access Point می باشد.

Association: فرآیند اتصال یک دستگاه وایرلس به Access Point را گویند.

HotSpot: محلهایی که شبکه های وایرلس در دسترسی عموم قرار دارند.

مدولاسیون: جهت انتقال دیتا به صورت بی سیم، نیاز به تولید یک موج سینوسی می باشد که بیت های دیتا را روی این موج های سینوسی سوار شده و ارسال می گردند. در طرف دیگر این بیت ها از روی موج سینوسی برداشته شده و دوباره سر هم می شوند. به موج سینوسی ، حامل (Carrier) و به سوار کردن بیت های دیتا بر روی این موج مدولاسیون (Modulation) می گوئیم. انواع مدولاسیون ها شامل DSSS ، FHSS و BPSK، QPSK، CCK، OFDM می باشد.

نکته: اطلاعات واقعی در یک سیگنال مدوله شده را sidebands می نامند.

### • انواع آنتن در شبکه های وایرلس

آنتن ها را می توان به دو رده کلی درون ساختمان Indoor و بیرون ساختمان Outdoor تقسیم بندی کرد. آنتن های بیرونی عموماً دارای جنس، پوشش و اتصالاتی هستند که بتوانند در شرایط دشوار فضای آزاد مثل باد، طوفان، برف، باران و سرما و گرمای شدید دوام بیاورند. در حالی که آنتن های درون ساختمان با ظاهر و پوشش ظریف و حتی الامکان زیبا ساخته می شوند تا باعث زشت شدن محیط داخلی ساختمان و دکوراسیون آن نشوند. آنتن های درونی را نمی توان در بیرون ساختمان نصب کرد مگر آنکه در مشخصات آن به صراحت به ویژگی (درونی/بیرونی) اشاره شده باشد.

به طور کلی در شبکه های وایرلس سه نوع آنتن وجود دارد که البته هر کدام دارای زیر مجموعه هایی می باشند.

✓ آنتن همه طرفه Omni Directional

✓ آنتن نیمه جهت دار Semi Directional

✓ کاملاً جهت دار Highly Directional



# فصل سوم

## مدل های مرجع

### ❖ OSI Reference Model

سازمان ISO یک سازمان استاندارد بین المللی است که استاندارد طیف وسیعی از محصولات گوناگون را تعیین می کند که از جمله این استانداردها مربوط به تجهیزات شبکه می باشد و مدل OSI نیز توسط این سازمان ارائه شد.

برای شناسایی هر چه بهتر کارکرد شبکه از مدل های مرجع استفاده می شود که مدل OSI یکی از مدل های مرجع است.

### ویژگی های مدل OSI (open system interconnection)

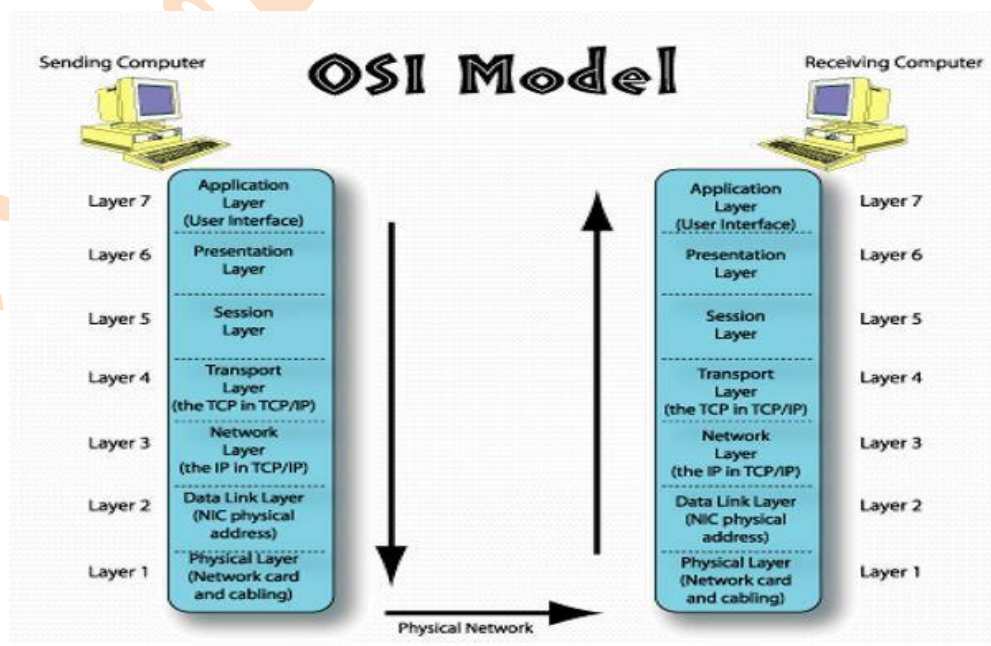
این مدل توسط سازمان ISO در سال ۱۹۸۴ ارائه گردید.

این مدل در هفت لایه ارائه شد.

هر لایه با لایه پایین تر در ارتباط است.

هر لایه دارای وظیفه خاصی است.

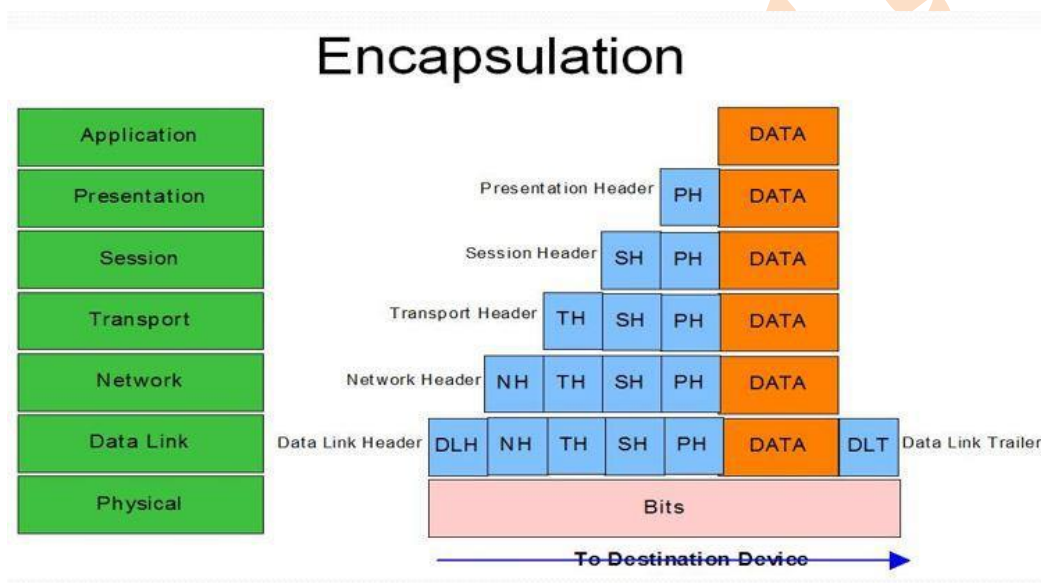
**پروتکل:** مجموعه ای از قوانینی که توسط کامپیوترها مورد استفاده قرار می گیرد تا کامپیوترها بتوانند با یکدیگر ارتباط برقرار کنند. پروتکل یک توافق استاندارد بوده که ارتباطات بر اساس آن صورت می گیرد در تصویر زیر انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر را مشاهده می نمایید.



## • کپسوله کردن اطلاعات (Data Encapsulation)

عمل بنیادی که پروتکل های موجود در لایه های مختلف مدل OSI انجام می دهند اضافه کردن هدر (Header) و در یک مورد خاص فوتر (Footer) به اطلاعاتی که از لایه بالایی خود می گیرند، می باشد.

به طور مثال درخواست دستیابی یک برنامه به منابع شبکه از لایه های پشته پروتکل می گذرد. زمانی که درخواست به لایه انتقال می رسد هدر مربوط به خود را به آن اضافه کرده و تحویل لایه شبکه می دهند. در این لایه هم هدرهای مخصوص اضافه شده و در لایه پیوند داده ها هم به همین صورت بوده و محصول نهایی به عنوان یک بسته برای انتقال آماده می شود. بعد از رسیدن این بسته به مقصد همین موارد فوق تکرار شده ولی این بار برعکس و رو به لایه هفتم که در هر لایه هدرها و فوترها مورد پردازش و حذف شده و پس از اتمام مراحل درخواست به برنامه مقصد در لایه هفتم با کاربرد می رسد. در واقع مفهوم کپسوله کردن فرآیندی است که در آن پروتکل های لایه های مختلف هدر و فوتر خود را به درخواست تولید شده توسط \*یک برنامه کاربردی اضافه می کنند.



## • لایه فیزیکی Physical layer:

اولین لایه مدل OSI بوده و در پایین ترین سطح این مدل است. در این لایه نحوه اتصال دو ایستگاه به یکدیگر از طریق کابل و توپولوژی های شبکه و سرعت آن ها توضیح داده می شود. این لایه مسئول تبدیل اطلاعات از بیت به سیگنال های الکتریکی می باشد. در واقع اگر بخواهیم موقعیت این لایه را نشان دهیم لبه کارت شبکه ما یعنی مابین کارت شبکه و رسانه انتقال (کابل و...) همان لایه فیزیکی می شود.

پارامترهایی که باید در این لایه مورد نظر باشند عبارتند از: ماهیت فیزیکی خط انتقال (مسی، فیبر نوری، میکروویو و ...) چگونگی نمایش بیت ها در قالب سیگنال متناسب با کانال ظرفیت کانال فیزیکی و نرخ ارسال (bit rate) مسائل مکانیکی و الکتریکی مانند نوع کابل، باند فرکانسی و نوع رابط کابل (کانکتور).

## • لایه پیوند داده ها Data link layer:

دومین لایه از مدل OSI می باشد که وظیفه این لایه آن است که با استفاده از مکانیزم ها کشف و کنترل خطا، داده را روی یک کانال بدلیل وجود نویز، بدون خطا به مقصد برساند.

در زمان انتقال اطلاعات ممکن است فریم خراب یا گم شود این وظیفه لایه پیوند داده‌هاست که در مقصد فریم را بررسی و خطایابی نماید وظیفه دیگر این لایه اطلاعات ارسالی از لایه بالاتر را به واحدهای استاندارد و مجاز تبدیل کرده و افزودن فیلدهای اطلاعاتی خاص (مثل آدرس مبدا، آدرس مقصد، کدهای کشف خطا و ...) یک فریم را تشکیل داده و برای لایه بعدی آماده می‌کند. این لایه خود از دو زیر لایه به نام‌های LLC و MAC تشکیل شده‌است. هر کدام از این زیرلایه‌ها وظایفی را به عهده دارند.

#### • زیرلایه LLC:

فریم‌بندی و شماره‌گذاری فریم‌ها و ارسال

دریافت فریم‌ها در کامپیوتر مقصد و بازسازی آن

فرستادن Acknowledge به فرستنده در صورت دریافت صحیح اطلاعات برای هر فریم

در صورت عدم ارسال Acknowledge از سوی گیرنده برای یک فریم آن فریم دوباره توسط فرستنده ارسال خواهد شد

#### • زیرلایه MAC:

این زیر لایه کنترل دسترسی رسانه نحوه و روش دسترسی یک ایستگاه به شبکه را بیان می‌دارد که دو نمونه از آن عبارتند از:

Token Pasing

(carrier sense multiple access / collision detection) CSMA/CD

روش Token Pasing:

جلوگیر از تصادم یا collision

حرکت یک بسته خالی از اطلاعات درون شبکه (Tok)

کامپیوتر برای ارسال اطلاعات منتظر Token می‌ماند.

اقدام به ارسال اطلاعات پس از رسیدن Token به کامپیوتر

باقی ماندن Token تا پایان ارسال کامل اطلاعات نزد کامپیوتر

عدم ارسال اطلاعات توسط کامپیوترهای دیگر

ارسال Acknowledge پس از پایان ارسال اطلاعات توسط کامپیوتر دریافت کننده به کامپیوتر مبدا

ایجاد یک Token توسط کامپیوتر مبدا و آزاد کردن آن در شبکه

روش CSMA/CD:

در این روش اگر دو کامپیوتر هم‌زمان اقدام به ارسال اطلاعات کنند تصادم رخ می‌دهد برای جلوگیری از این تصادم هر دو کامپیوتر ارسال را رها کرده و مدت زمانی به صورت تصادفی صبر کرده و سپس مجددا اقدام به ارسال اطلاعات می‌کنند.

### • لایه شبکه Network layer:

سومین لایه از مدل OSI می باشد که وظیفه مسیریابی و یافتن آدرس های مبدا و مقصد برای انتقال داده را به عهده دارد. پیچیده ترین لایه مدل OSI است چون عمل مسیریابی در آن انجام می شود. این لایه ترافیک شبکه را نیز کنترل کرده و با انتخاب مسیر جدید برای داده از بروز ترافیک جلوگیری می کند. پروتکل IP که از مهمترین پروتکل های شبکه است در این لایه قرار دارد که وظیفه آن آدرس دهی می باشد.

### • لایه انتقال Transport layer:

چهارمین لایه از مدل OSI می باشد که همانطور که از نامش پیداست وظیفه آن انتقال اطلاعات است. این لایه داده را از لایه بالاتر یعنی session گرفته و به قطعاتی با اندازه مناسب تقسیم کرده، اطلاعات مبدا و مقصد از قبیل شماره پورت به پاکت اضافه می کند و به لایه شبکه تحویل می دهد.

### • لایه نشست Session layer:

پنجمین لایه از مدل OSI می باشد در این لایه مانند لایه انتقال ارسال اطلاعات است اما خدمات پیشرفته ای نیز ارائه می کند در این لایه ارتباط بین دو ایستگاه با یک توافق آغاز می شود (Authentication , Authorization , login) و ادامه می یابد تا طی روالی هماهنگ پایان یابد. وظایف کلی این لایه:

برقراری و مدیریت یک نشست

شناسایی طرفین

حسابداری مشتری ها

اتمام نشست

### • لایه نشست Presentation:

ششمین لایه از مدل OSI می باشد در این لایه داده ها به روش استاندارد کد گذاری و قالب بندی می شوند.

برای اینکه کامپیوترهای با کدها و قالب بندی مختلف بتوانند داده ارسال کنند باید با استفاده از یک کدگذاری و قالب بندی استاندارد تبادل اطلاعات نمایند که برای سیستم عامل های مختلف قابل فهم باشد.

این لایه اطلاعات را از لایه بالایی یعنی لایه کاربرد گرفته و با شیوه کدگذاری استاندارد به شیوه قابل فهم برای کامپیوتر مقصد تبدیل کرده و به لایه جلسه تحویل می دهد.

### • لایه نشست Application layer:

هفتمین لایه از مدل OSI و همچنین بزرگترین لایه از این مدل می باشد. این لایه نقطه ورودی است برای دستیابی به مدل OSI است. تمام برنامه های شبکه در این لایه قرار دارند و ارتباط بین برنامه های روی شبکه در این لایه فراهم می گردد.

در این لایه خدمات سودمندی از قبیل ارسال فایل، کنترل یک کامپیوتر از راه دور و.... ارائه می گردد.

## • مدل TCP/IP:

برخلاف تصورات رایج مدل TCP/IP قبل از مدل OSI ارائه شد و در واقع مدل OSI برگرفته از مدل TCP/IP می باشد. این مدل یک ساختار چهار لایه ای دارد که لایه های آن به ترتیب زیر می باشد.

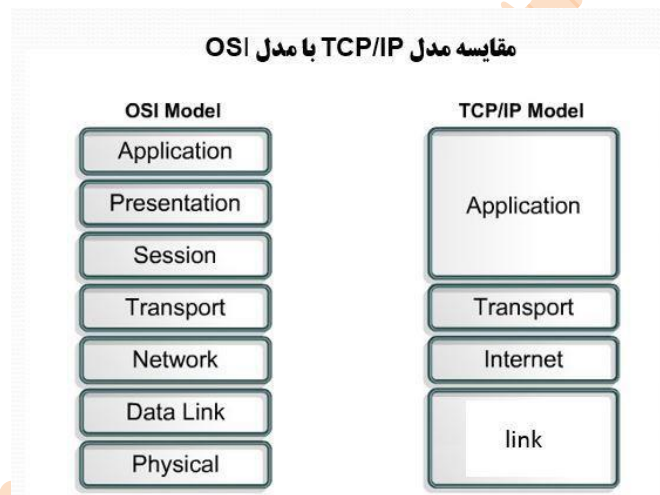
Link

Internet یا Ip

Transport

Application

نکته ای که در TCP/IP مهم است مفهوم مدل و پشته TCP/IP می باشد. مدل TCP/IP ساختاری چهار لایه دارد که به آن خواهیم پرداخت. پشته TCP/IP یا TCP/IP Protocol Stack مجموعه ای شامل بیش از صد پروتکل است که برای سازماندهی کلیه اجزای شبکه اینترنت به کار می رود که به این پروتکل ها در بخش های بعد می پردازیم.



## • لایه واسط شبکه Link:

در این لایه استانداردهای سخت افزاری و نرم افزارهای راه انداز تعریف می شود. این لایه درگیر با مسائل فیزیکی، کانال های انتقال، نوع کارت شبکه، نوع توپولوژی به کار رفته در شبکه است. این لایه معادل لایه های Data Link و Physical در مدل OSI می باشد.

## • لایه شبکه IP یا اینترنت:

وظیفه این لایه هدایت بسته ها از مبدا به مقصد می باشد. در این لایه چندین پروتکل وظیفه مسیریابی و تحویل بسته های اطلاعاتی را از مبدا به مقصد انجام می دهند.



این لایه معادل لایه Network در مدل OSI می باشد.

پروتکل های این لایه عبارتند از:

IP

ICMP

IGMP

ARP

RARP

لایه انتقال Transport:

وظیفه این لایه انتقال می باشد که معادل لایه انتقال در مدل OSI است.

در این لایه پروتکل های TCP و UDP فعالیت می کنند.

اتصال گرا بودن و بدون اتصال بودن نیز در این لایه تعریف می گردد.

دو نوع پروتکل در این لایه ارائه می گردد:

اتصال گرا connection oriented: در این پروتکل ابتدا ارتباط برقرار می شود بعد داده ارسال می گردد. (TCP)

بدون اتصال connection less: در این پروتکل نیازی به برقراری ارتباط قبل از ارسال داده نیست. (UDP)

#### • لایه کاربرد Application:

در این لایه بر اساس خدمات لایه های زیرین، سرویس سطح بالایی برای خلق برنامه های کاربردی ارائه می شود.

این خدمات در قالب خدمات وب، انتقال صفحه های اینترنتی، مدیریت پست الکترونیکی و... است.

پروتکل های این لایه هم عبارتند از:

HTTP

FTP

POP۳

TELNET

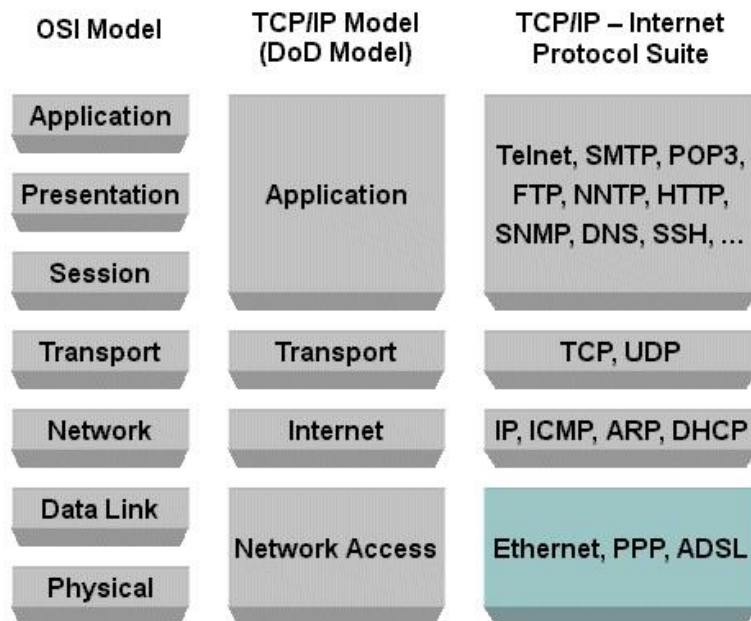
DNS

DHCP



## پروتکل های مدل TCP/IP:

در این بخش به آشنایی با پروتکل های مدل TCP/IP خواهیم پرداخت. در تصویر زیر برخی از این پروتکل ها را مشاهده می نمایید.



به علت اهمیت پروتکل IP و به دلیل اینکه در تمام پروتکل و سرویس های ارائه شده در شبکه IP نقش مهمی را ایفا می کند، ابتدا به این پروتکل می پردازیم.

## Internet Protocol یا IP:

این پروتکل یکی از مهمترین پروتکل های شبکه بوده و وظایف مهمی را بر عهده دارد که عبارتند از:

کپسوله کردن: روند بسته بندی داده ها

آدرس دهی: تشخیص سیستم های موجود در شبکه به وسیله آدرس IP

مسیریابی: تشخیص بهترین مسیر تا سیستم مقصد

قطعه بندی: بخش کردن داده ها به قطعه هایی با اندازه مناسب برای انتقال در شبکه

همانطور که در قسمت کپسوله سازی در مدل OSI توضیح داده شد، در هر لایه یک هدر به بسته اصلی اضافه خواهد شد. این هدر در لایه شبکه و برای پروتکل IP به شکل زیر خواهد بود.

4-bit	8-bit	16-bit	32-bit	
Ver.	Header Length	Type of Service	Total Length	
Identification			Flags	Offset
Time To Live	Protocol	Checksum		
Source Address				
Destination Address				
Options and Padding				

فیلد Version: اولین فیلد در هدر IP می باشد که ۲ بیت است که نسخه پروتکل IP که این بسته بر اساس آن سازماندهی و ارسال شده است را تعیین می کند. امروزه با توجه به ارائه نسخه ۶ از این پروتکل ولی هنوز مشاهده می شود که اکثرا در شبکه های اینترنت و داخلی از نسخه ۲ این پروتکل استفاده می نمایند. در قسمت های بعد به تفصیل در مورد نسخه های این پروتکل توضیح داده خواهد شد.

فیلد IP Header Length یا IHL: در این فیلد که ۲ بیتی است، طول کل سرآیند بسته را مشخص می نماید.

فیلد Type of Service: این فیلد ۸ بیتی است که توسط آن، ماشین میزبان (ماشین تولید کننده بسته IP) از مجموعه مسیریاب ها تقاضای سرویس ویژه ای برای ارسال یک دیتاگرام را می نماید.

فیلد Total Length: در این فیلد ۱۶ بیتی عددی قرار می گیرد که طول کل بسته که شامل IP و هدر است. حداکثر طول کل بسته IP می تواند ۶۳۳۲۳ بایت باشد.

**فیلد Total Length:** در این فیلد ۱۶ بیتی عددی قرار می گیرد که طول کل بسته IP را که شامل مجموع اندازه سرآیند و ناحیه داده است، تعیین می کند. مبنای طول بر حسب بایت است و بنابراین حداکثر طول کل بسته IP می تواند ۶۵۵۳۵ بایت باشد.

فیلد Identification: با توجه به اینکه در برخی مواقع ماشین های میزبان یا مسیریاب ها مجبورند بسته را به قطعات کوچکتری تقسیم کنند، هر قسمت شکسته شده باید دارای مشخصه ای برای شناسایی باشد. عددی که در این فیلد ۰۶ بیتی عددی قرار می گیرد که شماره یک دیتاگرام واحد را مشخص می کند. کلیه بسته های IP که با این شماره وارد می شوند قطعه های مربوط به یک دیتاگرام بوده و و باید پس از گردآوری، بازسازی شوند.

فیلد Fragment Offset: این فیلد خود دارای سه بخش است:

۱- بیت Don't Fragment یا DF: با یک شدن این بیت در یک بسته IP هیچ مسیریابی حق قطعه قطعه کردن آن را ندارد، چرا که مقصد قادر به بازسازی دیتاگرام های تکه تکه شده نیست. اگر این بیت به یک تنظیم شده باشد و مسیر یاب نتواند آن را به دلیل بزرگی اندازه، انتقال دهد لاجرم حذف خواهد شد.

۲- بیت More Fragment یا MF: این بیت مشخص می کند که آیا بسته IP آخرین قطعه از یک دیتاگرام محسوب می شود یا باز هم قطعه بعدی وجود دارد. در آخرین قطعه از یک دیتاگرام بیت MF صفر خواهد بود و در بقیه الزاما یک است.

۳- بیت Fragment Offset: این قسمت که ۰۲ بیتی است در حقیقت شماره ترتیب هر قطعه در یک دیتاگرام شکسته شده را مشخص می نماید. با توجه به حداکثر ۰۲ بیتی بودن این فیلد، یک دیتاگرام حداکثر می تواند به ۸۰۱۳ تکه تقسیم شود. نکته مهم در

این فیلد آن است که اندازه هر قطعه باید ضربی از ۸ باشد. یعنی به استثنای قطعه آخر، اندازه بقیه قطعه ها بایستی به گونه ای انتخاب شود که ضربی از ۸ باشد.

به عنوان مثال فرض کنید مسیریابی مجبور است یک دیتاگرام را به طول ۳۱۱۱ بایت قطعه قطعه کند به گونه ای که اندازه هر قطعه کمتر از ۰۳۱۱ بایت باشد. در این حالت نمی تواند اندازه هر قطعه را ۰۳۳۱ در نظر بگیرد چرا که ضربی از ۸ نیست ولی اندازه ۰۳۸۱ مناسب می باشد. بر این اساس مسیریاب، دیتاگرام را به سه بسته ۰۳۸۱ بیتی و یک بسته ۰۰۶۱ بیتی می شکند. در این مثال فرض کنید مسیریاب عدد ۳۲۳۳ را به عنوان مشخصه دیتاگرام انتخاب کرده است. بنابراین برای هر یک از ۲ قطعه دیتاگرام، فیلد آفست و مشخصه به صورت زیر است.

طول هر قطعه	آدرس محل قرار گرفتن قطعه در دیتاگرام	بیت MF	Fragment Offset	Identification	شماره قطعه
۱۲۸۰	$8 * 0 = 0$	۱	۰	۲۳۲۲	قطعه شماره ۱
۱۲۸۰	$8 * 160 = 1280$	۱	۱۶۰	۲۳۲۲	قطعه شماره ۲
۱۲۸۰	$8 * 320 = 2560$	۱	۳۲۰	۲۳۲۲	قطعه شماره ۳
۱۱۶۰	$8 * 480 = 3840$	۰	۴۸۰	۲۳۲۲	قطعه آخر

فیلد Time To Live: این فیلد ۸ بیتی در نقش یک شمارنده، طول عمر بسته را مشخص می کند. طول عمر یک بسته به زمانی اشاره می کند که بسته IP می تواند بر روی شبکه سرگردان باشد. حداکثر طول عمر یک بسته ۳۳۳ خواهد بود که به ازای عبور از هر مسیریاب از مقدار این فیلد یک واحد کم می شود. هر گاه یک بسته IP به دلیل بافر شدن در حافظه یک مسیریاب زمانی رامعطل بماند، به ازای هر ثانیه یک واحد از این فیلد کم خواهد شد. حال اگر مقدار این فیلد به صفر برسد بسته IP در هر نقطه از مسیریاب باشد، حذف می گردد. البته پس از حذف یک هشدار به ماشین تولید کننده ارسال خواهد شد.

فیلد Protocol: دیتاگرامی که در فیلد داده از یک بسته IP حمل می شود با ساختمان داده خاص از لایه بالاتر تحویل پروتکل IP شده تا روی شبکه ارسال شود. به عنوان مثال ممکن است این داده ها را پروتکل TCP در لایه بالاتر ارسال کرده باشد و یا ممکن است این کار توسط پروتکل UDP انجام شده باشد. بنابراین مقدار این فیلد شماره پروتکلی است که در لایه بالاتر تقاضای ارسال یک دیتاگرام کرده است. بسته ها پس از دریافت در مقصد باید به پروتکل تعیین شده تحویل داده شوند.

فیلد Header Checksum: این فیلد که ۰۶ بیتی است به منظور کشف خطاهای احتمالی در سرآیند هر بسته از IP استفاده می شود. برای محاسبه کد کشف خطا، کل سرآیند به صورت دو بایت، دو بایت با یکدیگر جمع می شود. نهایتاً حاصل جمع به روش مکمل منفی می شود و این عدد منفی در این فیلد قرار می گیرد. در هر مسیریاب قبل از پردازش و مسیریابی ابتدا صحت اطلاعات درون سرآیند بررسی می شود. دقت کنید که فیلد Checksum در هر مسیریاب باید از نو محاسبه و مقدار دهی شود زیرا وقتی یک بسته IP وارد یک مسیریاب می شود حداقل فیلد TTL از آن بسته عوض خواهد شد.

فیلد Source Address: هر ماشین میزبان در شبکه اینترنت یک آدرس جهانی و یکتای ۲۳ بیتی دارد (البته ۲۳ بیت برای نسخه ۲ از IP بوده و نسخه ۶ آن ۰۳۸ بیتی می باشد). بنابر این هر ماشین باید در هنگام تولید یک بسته IP آدرس خودش را در این فیلد قرار دهد.

فیلد Destination Address: در این فیلد آدرس مربوط به مقصد که باید بسته IP به آن تحویل داده شود، قرار می گیرد.

فیلد اختیاری Options: در این فیلد اختیاری می تواند تا حداکثر ۲۱ بایت قرار داد که برای آزمایش، دیباگ، امنیت و سایر پارامترهای مشابه روی شبکه مورد استفاده قرار می گیرد.

فیلد Payload: در این فیلد داده های دریافتی از لایه بالاتر قرار می گیرد.

در پایان این پست از تمامی دوستانی که قصد ورود به دنیای امنیت و نفوذ را دارند تقاضا می کنم که مطالب این پست را به دقت مطالعه نمایند. چرا که تسلط بر این موضوع و موضوعات مربوط به TCP/IP که در ادامه به آن اشاره خواهیم نمود، از ضروریات ورود به عرصه امنیت و نفوذ است.

به طور مثال با دستکاری فیلدها می توان حملات مربوط به انکار سرویس یا DoS را انجام داد و یا اینکه برخی از ابزارهای پویش یا اسکن از فیلدهای TTL استفاده می کنند.

لازم به ذکر است که اکثر مطالب پست حاضر از کتاب نفوذگری در شبکه و روش های مقابله جناب احسان ملکیان برگرفته شده و قسمتی از آن هم مربوطه به سایت itpro.ir می باشد.

### سیستم آدرس دهی IP:

آدرس IP برای هر کامپیوتر (هر کارت شبکه) واحد می باشد که این آدرس در فیلدهای آدرس IP مبدا و مقصد هدر قرار می گیرد و هر کامپیوتر در شبکه یا اینترنت با این IP شناخته می شود.

طول آدرس IP، ۳۲ بیت یا ۴ بایت می باشد که به چهار قسمت ۸ بیتی تقسیم می شود (به هر قسمت ۸ بیتی یک Octet گفته می شود).

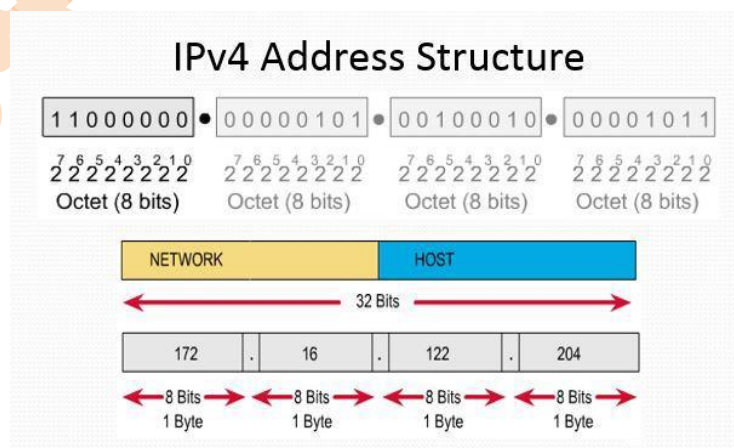
نکته: موارد ذکر شده مربوط به IPv۴ بوده و IPv۶ بوده که ۱۲۸ بیتی است و در آخر توضیح داده می شود.

که IP را به صورت ۲ عدد در مبنای دهدهی می نویسند که هر یک از این ۲ عدد بین صفر تا ۳۳۳ می باشند.

255,255,255,255,1,1,1,1

192.168.1.10

هر آدرس IP از دو قسمت شناسه شبکه (Network ID) و شناسه میزبان (Host ID) می باشد که این دو در کلاس های مختلف IP تفاوت دارد.



آدرس IP طبق مثال قبل به صورت دسیمال یا دهدهی می باشد ولی زبانی که برای کامپیوتر قابل فهم است زبان باینری یا همان صفر و یک است.

کلاس های IP:

شرکت IANA(Internet Assigned Numbers Authority) شرکتی است که وظیفه تخصیص IP در اینترنت را دارد تا هیچ دو IP در اینترنت یکسان نباشد.

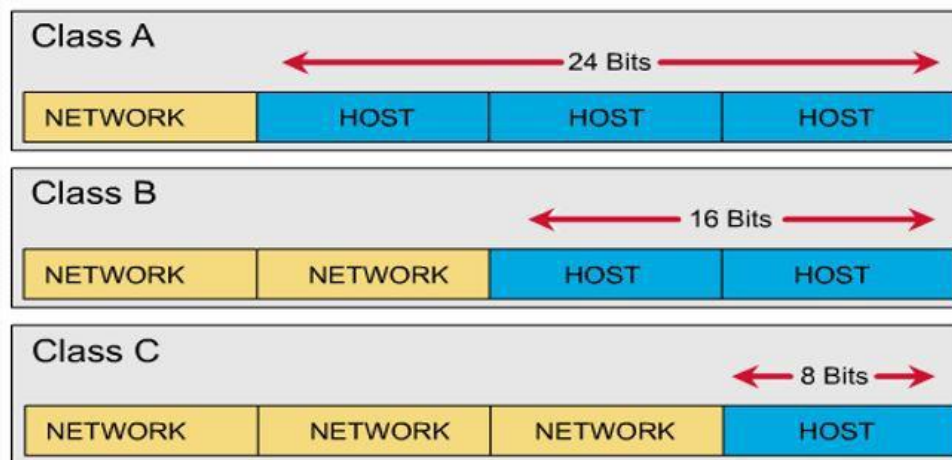
IANA کلاس بندی هایی را به منظور استفاده از IP ها ارائه داده است که تمام شبکه ها موظف به تبعیت از آن هستند.

IPv۴ به ۵ کلاس A,B,C,D,E تقسیم بندی می شود.

کلاس بندی IP به شکل زیر می باشد:

Class	IP	Subnet Mask	First bit	Net ID bit	Host ID bit	Number of Net	Number of Host
A	1-126	255.0.0.0	0	8	24	$2^7-2$	$2^{24}-2$
B	128-191	255.255.0.0	10	16	16	$2^{14}$	$2^{16}-2$
C	192-223	255.255.255.0	110	24	8	$2^{21}$	$2^8-2$
D	224-239	---					
E	240-254	---					

## IPv4 Class Structure



Public & private IP

Public IP: به آدرس IP گفته می شود که جنبه عمومی داشته و در اینترنت معتبر می باشد.

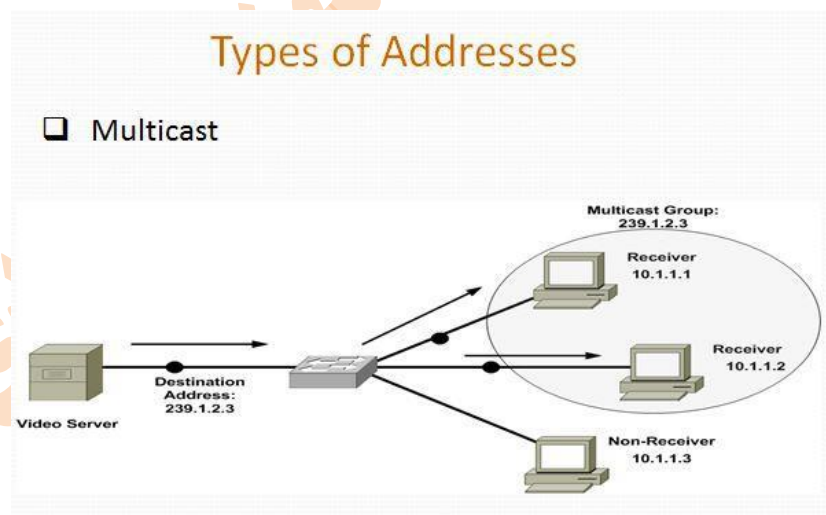
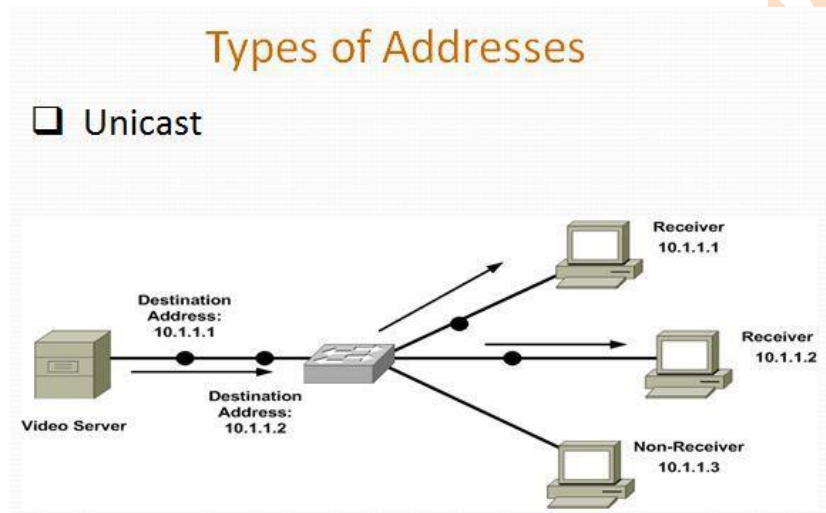
Private IP: به آدرس IP گفته می شود که در شبکه های محلی مورد استفاده قرار می گیرد.

Class	IP	Subnet Mask	Private IP Address
A	1-126	255.0.0.0	10.0.0.1-- 10.255.255.254
B	128-191	255.255.0.0	172.16.0.1– 172.31.255.254
C	192-223	255.255.255.0	192.168.0.1 – 192.168.255.254

### • انواع آدرس دهی در شبکه:

در ساختار شبکه و آدرس دهی، سه نوع ارتباط وجود دارد که شامل آدرس های تک پخشی یا Unicast، چند پخشی یا Multicast و همه پخشی یا Broadcast می باشد. به طور مثال شما می خواهید به پیامک به یکی از دوستان خود فرستاده و تولد او را تبریک بگویید که در واقع ارسال یک به یک یا همان Unicast را انجام داده اید. اگر برای یک جلسه بخواهید چند نفر از دوستانتان را دعوت کنید آنگاه در گوشی خود یک گروه ساخته و پیامک دعوت به جلسه را به آن ها ارسال می کنید که این در واقع ارسال به صورت Multicast یا یک به چند است. اگر بخواهید عید نوروز را به همه دوستان تبریک بگویید به پیامک را send to all می کنید که این ارسال همان Broadcast است.

به تصاویر زیر توجه کنید.



ای پی نسخه ۶:

یکی از مشکلات نسخه چهار، تعداد کم آپی آدرس است. مقدار هر یک از این چهار بخش که با نقطه از هم جدا شده اند، بین صفر و ۲۵۵ است که با این ترتیب حدود چهار میلیارد آپی آدرس قابل استفاده در این نسخه وجود دارد. به سادگی می توان در یک نظر تفاوت بین IPv ۶



و ۴ IPv را تشخیص داد. یک آدرس ۶ IPv از ۱۲۸ بیت برای آدرسهی استفاده می کند که با این ترتیب حدود ۲ به توان ۱۲۸ آدرس عددی ۳۹ رقمی خواهیم داشت و به نظر نمی رسد با این مقدار آدرس تا چند دهه آینده دچار کمبود آبیی آدرس شویم.

حال برای درک آبیی آدرس نسخه ۶، هر ۱۶ بیت را به صورت شانزده تایی یا همان هگزادسیمال می\*نویسیم و با علامت کولن (: ) آن ها را از هم جدا می کنیم.

P نسخه ۶ عددی ۱۲۶ بیتی است و بر مبنای هگزا دسیمال می باشد. دارای ۸ Octet است که هر کدام ۱۶ بیت است ۶ IPv. دارای Prefix است.

نمونه ای از IP نسخه ۶ را در زیر مشاهده می نمایید. که در آن هر قسمت با : از هم جدا شده اند. در ساختار IP نسخه ۶ به جای

Subnet mask

Prefix جایگزین شده است.

A3C38:1FF:FE11AA:8:1111:1111:13FB3110:1

شما برای راحتی و خوانایی نمونه هایی از این دست IP نسخه ۶ می توانید صفرهای قبل از اعداد در بین : را حذف نمایید. همچنین در صورتی که تمامی اعداد در یک قسمت صفر بود، به جای ۲ صفر می توان از یک صفر استفاده کرد. در این صورت نمونه بالا به نمونه ای که در زیر آمده است، تبدیل خواهد شد.

A3C38:1AA:FF:FE8:1:1:3:FB3110

باز هم برای خوانایی IP شما می توانید قسمت هایی که صفر هستند را حذف نموده و خالی بگذارید. به نمونه زیر توجه کنید.

A3C38:1AA:FF:FE3::8:FB3110

نکته: اساس کار در شبکه های بر مبنای IP نسخه ۶، نام می باشد ساختار یک به یک در این IP به شکل زیر است.

Global

معادل همان Public در نسخه ۲ است. این نوع IP با ۱۱۰ شروع می شود.

Link-Local

معادل apipa در نسخه ۲ است. این IP با fe شروع می شود.

Site-local

معادل Private در نسخه ۲ است. این IP با fec شروع می شود.

Special

معادل Loop Back در نسخه ۲ است. به صورت :: نشان داده می شود.

• مسیریابی یا Routing

یکی از پیچیده ترین عملکردهای شبکه، انجام فرآیند مسیریابی می باشد. این عمل در لایه سوم از مدل OSI یعنی شبکه یا Network صورت می گیرد. مطالب زیادی در زمینه مسیریابی در کتب مختلف نوشته شده است ولی در این قسمت از دوره Network بیشتر به بحث اولیه آن می پردازیم و مباحث پیشرفته و همچنین پیاده سازی این ساختار در دوره هایی مانند CCNA و CCNP به طور کامل بررسی می گردد.

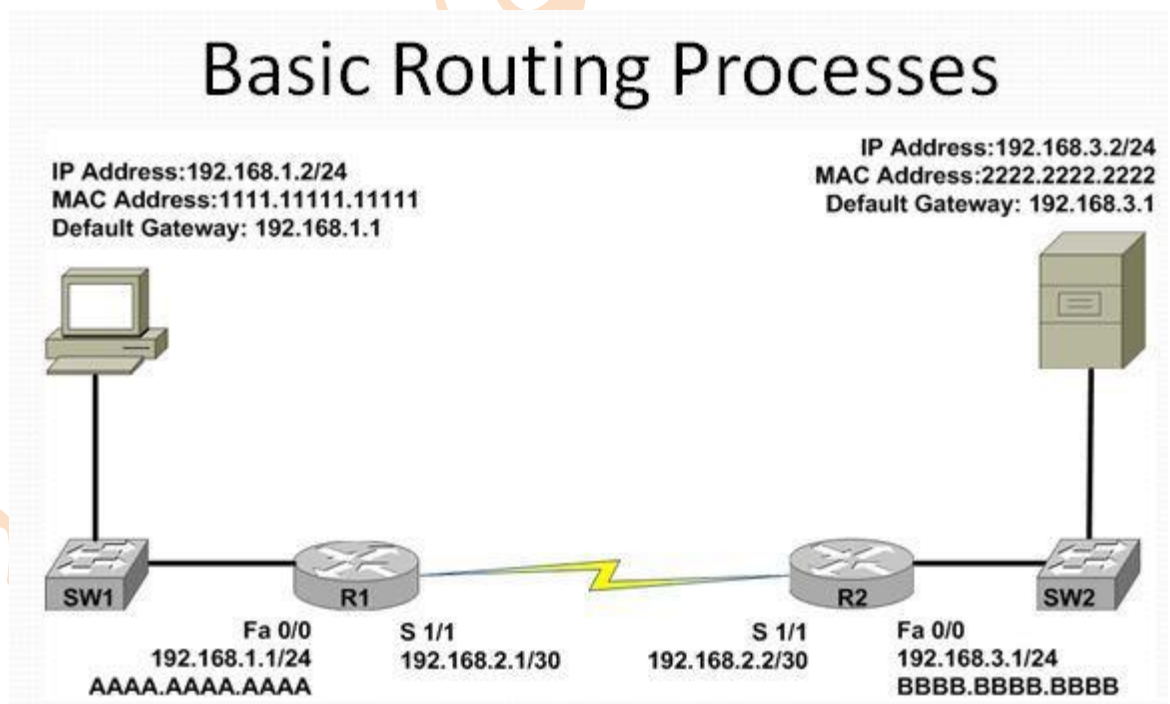
عملیات Routing می تواند توسط یک دستگاه لایه سه مانند Router و یا یک سرور میکروسافت که سرویس RAS و RRAS روی آن نصب شده باشد، در سطح شبکه صورت گیرد.

این دستگاه ها و عملیات مسیریابی زمانی در شبکه رخ می دهد که ناهمگونی در زیر شبکه و یا آدرس IP متفاوتی در شبکه بوجود آمده و بخواهیم بسته های را از اصطلاح Broadcast Domain خارج کنیم و به شبکه دیگری وارد نماییم.

این مورد را با یک مثال توضیح می دهیم.

فرض کنید شما داخل منزل خودتان هستید. اگر بخواهید یکی از افراد خانه را صدا بزنید، او جواب شما را می دهد و نیازی به رفتن به جایی خارج از خانه نیست. حال شما می خواهید یک مطلبی را به همسایه خود بگویید باید ابتدا از خانه خارج شده و درب خانه وی را زده و پس از دیدن وی، مطلب مورد نظر را به وی منتقل کنید.

فرآیند مسیریابی هم تقریباً به همین صورت است ولی نه به همین راحتی!!!!!! اگر شما بخواهید داخل بازه شبکه خود یا اصطلاحاً در یک Subnet ارتباط برقرار کنید، نیازی به خارج شدن از شبکه و استفاده از روتر نیست. ولی اگر بخواهید با یک شبکه با رنج متفاوتی از IP و Subnet ارتباط برقرار کنید، نیازمند یک دستگاه واسط برای انجام عمل مسیریابی می باشید. به شکل زیر توجه نمایید



برای ارتباط با یک شبکه دیگر شما نیاز به داشتن روتر یا مسیریاب دارید. وظیفه این دستگاه انجام عمل مسیریابی و ارسال بسته اطلاعات از یک سمت شبکه یا یک گوش (Interface) خود به سمت دیگر شبکه یا گوش دیگر خود است. پس از تنظیماتی که باید در مسیریاب صورت پذیرد شما باید بر روی کلاینت های خود در قسمت تنظیمات کارت شبکه IP کارت شبکه سمتی از روتر که طرف کلاینت است را به عنوان Default Gateway قرار دهید. در مقصد هم این کار باید صورت پذیرد



عملیات مسیریابی به روش های مختلفی انجام می گردد. این روش ها بیشتر به دو قسمت Static و Dynamic دسته بندی می شوند. در روش ایستا شما باید به صورت دستی جداول مسیریابی را تنظیم نمایید و ساختار آن را به شکل مورد نظر خود پیکربندی نمایید (ساختار آن در دوره CCNA بحث می شود). این کار شاید زمانی که شما یک یا چند مسیریاب داشته باشید، راحت به نظر برسد. اما زمانی که تعداد روترها در بین را بیشتر می شود استفاده از ساختار ایستا بسیار زمان بر بوده و در برخی موارد با مشکل پیکربندی نادرست مواجه می شود. در روش پویا یا Dynamic شما راهکار راحتی تری پیش رو دارید و با استفاده از پروتکل های مسیر یابی مختلف می توانید به راحتی مسیریابی را با صرف وقت کمتر انجام دهید. نمونه ای از این پروتکل ها به ترتیب زیر است:

RIP (Router Information Protocol )

OSPF (Open Shortest Path First )

EIGRP (Enhanced Interior Gateway Routing Protocol )

BGP (Boarder Gateway Protocol )

در انجمن فیلمی به همراه صدا قرار داده شده است که در محیط برنامه Packet Tracer یک ساختار مسیر یابی توضیح داده می شود. برنامه Packet Tracer به منظور شبیه سازی دستگاه های شرکت سیسکو طراحی شده است و محیط البراتور برای تست دستورات سیسکو و آموزش های آن است.

NAT (Network Address Translate)

همانطور که در بخش قبل در مورد مسیریابی توضیح دادم، زمانی که بخواهیم ارتباط به صورت دو طرفه برقرار شود از ساختار Route استفاده می شود. البته شاید این تعریف در نگاه اول درست به نظر نرسد ولی اگر ارتباط Route را از نوع دو طرفه مطرح کنیم، یعنی هم مبدا و هم مقصد بتوانند با یکدیگر ارتباط داشته و قادر به تبادل اطلاعات باشند، آنگاه NAT را می توان یک ارتباط یک طرفه تعریف کرد. به صورتی که زمانی که NAT را پیاده سازی می کنیم، شم دارای یک IP عمومی یا Public در اختیار دارید و مابقی IP ها به صورت Private می باشند. در این صورت شما قصد دارید تا از طریق IP عمومی به سیستم هایی که IP خصوصی دارند، اینترنت بدهید.

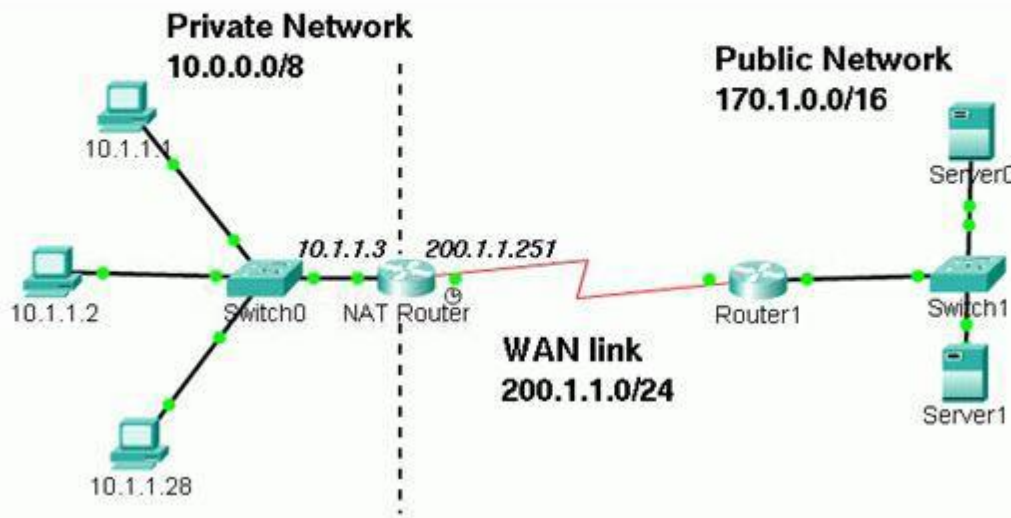
به منظور پیاده سازی چنین پروژه ای از ساختار NAT استفاده می گردد.

همانطور که از نام این پروتکل مشخص است، وظیفه آن ترجمه آدرس IP می باشد. در مثال فوق تمامی درخواست های ارسالی از داخل شبکه به وسیله IP های خصوصی به سمت روتر هدایت شده و از آنجا به IP عمومی ترجمه شده و به اینترنت و مقصد مورد نظر ارسال می شود. در این صورت تمام کاربران شبکه داخلی با یک IP عمومی وارد اینترنت می شوند. یکی از دلایل استفاده از NAT بحث صرفه جویی در استفاده از IP می باشد. به صورتی که در فوق مشخص شد، ما با یک IP به چندین نفر اینترنت دادیم و از IP دیگری استفاده نکردیم.

یکی از دلایل دیگر، بحث امنیت است. در صورتی که شما از NAT استفاده نمایید، ارتباط به صورت یک طرفه برقرار است. یعنی شما قادر خواهید بود مقصدی در اینترنت را مشاهده نموده و به آن پیامی ارسال کنید و مستقیماً با آن در ارتباط باشید. حال آنکه از خارج از شبکه شما کسی قادر به ارتباط مستقیم با شما نیست. اکثر ساختارهای اینترنت های خانگی بدین صورت است و به همین خاطر است زمانی که شما IP اصلی خود را پیدا می کنید و آن را در مروگر وارد می کنید با صفحه \*الگین مودم مواجه می شوید و نمی توانید به سیستمی که پشت NAT است به صورت مستقیم Remote Desktop بزنید.

تصویر زیر نمونه‌ای از ساختار NAT در شبکه است.

# Network Address Translation(NAT)



مواردی که گفته شد، گوشه از کاربرد های NAT در ساختار شبکه بوده و شما در محیط واقعی شبکه و ساختار ارتباطی به کاربرد های دیگر آن مواجه خواهید شد.

## • پروتکل ICMP (Internet Control Message Protocol)

این پروتکل در کنار پروتکل IP برای بررسی انواع خطا و ارسال پیام برای مبدا بسته در هنگام بروز اشکالات ناخواسته استفاده می‌شود. در واقع ICMP یک سیستم گزارش خطاست

چون ICMP خود درون یک بسته IP جاسازی می‌شود بنابراین فیلد پروتکل در سرآیند بسته IP باید باشماره مشخصه پروتکل ICMP تنظیم شود.

کار دیگر ICMP حمل درخواست‌های گوناگون برای دریافت اطلاعات به سیستم‌های دیگر و برگرداندن جواب های حاوی آن اطلاعات است . PING یک ابزار کمکی در این پروتکل است که با زدن این دستور به همراه IP مقصد در محیط CMD تعداد ۲ پکت ارسال می‌کند و مشخص کننده برقراری ارتباط بین دستگاه مبدا و مقصد می‌باشد.

Ping 10.0.0.1

از این دستور برای تست برقراری ارتباط استفاده می‌شود. هنگامی که این دستور را در محیط CMD وارد می‌کنید، اگر ارتباط برقرار باشد با پیغامی شبیه زیر مواجه می‌شوید

Reply from ۲۱۶.۲۳۹.۳۱۲.۲: bytes=۲۳ time=۰۱۱ ms TTL=۲۱

خط بال بدین معنی است که پاسخ از آدرس ۲۱۶.۲۳۹.۳۱۲.۲ دریافت شده‌است. حجم بسته‌ای که از آدرس مقصد دریافت شده‌است 32 بایت است. زمانیکه طول کشیده تا پاسخ دریافت شود 199 میلی ثانیه بوده‌است. TTL که مخفف Tim to live است

در بخش مربوط به سرآیند IP توضیح داده شده است. این جا این عدد برابر ۴۰ می باشد. به صورت پیش فرض اگر مقصد از سیستم عامل لینوکس استفاده نماید این عدد ۶۴ است. اگر از ویندوز استفاده کرده باشد، این عدد ۱۲۸ است و اگر از سخت افزارهای سیسکو استفاده شده باشد، این عدد ۲۵۶ می باشد.

نکته ای که باید به آن توجه کرد این است که در هنگام برقراری ارتباط به ازای هر گام در شبکه که همان روتر است، یک عدد از عدد پیش فرض کم می شود و هرگاه به صفر برسد بسته از چرخه ارتباط حذف شده و یک پیام به مبدا ارسال می شود. در جدول زیر برخی از پیام های مربوط به ICMP را مشاهده می نمایید.

مفهوم خطا	نام خطا
عدم در دسترس بودن شبکه	No unreachable
عدم در دسترس بودن میزبان	Host unreachable
عدم در دسترس بودن پورت	Port unreachable
شبکه مقصد ناشناخته است	Destination Network Unknown
ارتباط با شبکه مقصد توسط مدیر شبکه منع شده است	Communication With Destination Network Is Administrator Prohibited

#### • ARP (Address Resolution Protocol)

کار پروتکل ARP تبدیل آدرس IP به MAC بوده و با ارسال بسته های Broadcast در سطح شبکه، آدرس های MAC ماشین های داخل شبکه را شناسایی می کند. هنگامی که یک ماشین نیاز به برقراری ارتباط با دیگران داشته باشد، به جدول ARP مراجعه می کند. اگر آدرس MAC در این جدول پیدا نشد، پروتکل ARP یک بسته Broadcast را برای شناسایی آن درون شبکه پخش می کند.

در واقع در جدول ARP برای هر IP آدرس MAC آن مشخص شده است.

یک کامپیوتر هنگامی که بسته های ARP Request و ARP Reply را دریافت می نماید، حافظه ARP یا ARP Cache خود را بروز رسانی می نماید. یک میزبان در یک شبکه LAN می تواند بسته های ARP را به راحتی جعل نماید زیرا پروتکل ARP نیازی به احراز هویت ندارد. نفوذگر می تواند این نقض ذاتی را به عنوان یک مزیت در نظر گرفته و کامپیوترهای داخل شبکه را مورد حمله قرار دهد.

برای مدیریت این پروتکل می توان از دستورات خط فرمان کمک گرفت.

برای دیدن لیست مک های حافظه ای آر پی

ARP -a IP

محتویات حافظه ARP کارت شبکه ای را نشان می دهد که توسط آی پی مشخص شده است

ARP -n IP

برای اضافه کردن یک مک به حافظه‌ای آر پی

ARP –s IP MAC

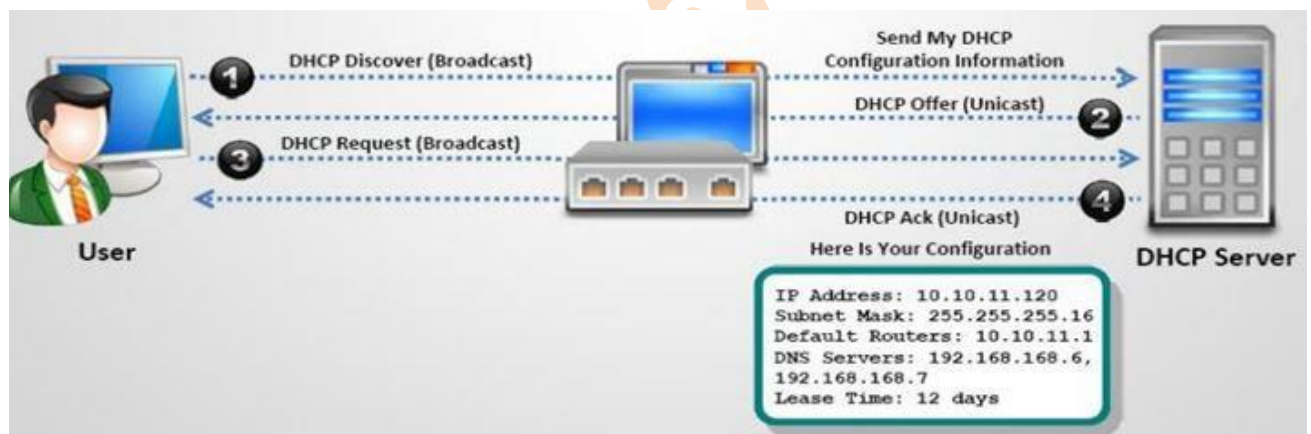
برای پاک کردن یک مک از حافظه‌ای آر پی

ARP –d IP

### • DHCP(dynamic host configuration protocol)

از این پروتکل برای دادن IP به صورت اتوماتیک استفاده می‌شود.

هنگامی که سرور DHCP بال بوده و به سوییچ متصل است و کاربر هم به سوییچ متصل شده و حالت تنظیم IP خود را در حالت اتوماتیک قرار دهد، یک بسته Broadcast توسط کاربر در شبکه با عنوان DHCP Discover پخش می‌شود. این بسته بدین معنی است که کاربر به دنبال سرور DHCP می‌گردد. هنگامی که این بسته به سرور DHCP رسید، سرور آن را تحویل گرفته و یک بسته Unicast به عنوان DHCP Offer به سمت کاربر ارسال می‌کند. این بسته بدین معنی است که سرور DHCP خود را به کاربر معرفی می‌کند. کاربر پس از دریافت این بسته، یک بسته Broadcast به عنوان DHCP Request را در سطح شبکه پخش خواهد کرد که بیانگر آمادگی برای گرفتن IP اتوماتیک است. در این زمان سرور DHCP پس از دریافت بسته DHCP Request یک بسته Unicast با عنوان DHCP Ack را به سمت کاربر ارسال می‌کند که این بسته حاوی اطلاعات مربوط به IP اتوماتیک برای کاربر است.



### • پروتکل های لایه Transport

دو پروتکل مهم که در این لایه کار می‌کنند عبارتند از:

#### TCP(Transmission Control Protocol)

این پروتکل یک پروتکل اتصال گرا (Connection Oriented) می‌باشد بدین معنی که ابتدا ارتباط برقرار شده و سپس داده ارسال می‌شود و این پروتکل نیز به بسته اطلاعاتی تحت عنوان هدر (Header) اضافه می‌کند.

در این پروتکل ایجاد یک ارتباط TCP معروف به دست تکانی سه مرحله‌ای (three way handshake) می‌باشد.

در این پروتکل صحت دریافت داده‌ها مشخص می‌گردد و دارای امنیت بیشتری نسبت به UDP می‌باشد.

### • Three-Way Handshake یا دست تکانی سه مرحله ای

TCP که یکی از پروتکل های مهم شبکه است، برای برقراری ارتباط بین دو دستگاه مانند کلاینت و سرور، از روشی به نام دست تکانی سه مرحله ای یا Three-Way Handshake استفاده می کند. مراحل این دست تکانی به شکل زیر است.

**مرحله اول :** در این مرحله سیستم اول بسته ای را که فقط flag SYN در آن تنظیم شده است، به سیستم دوم ارسال می کند. (درخواست برقراری ارتباط)

**مرحله دوم:** در این مرحله سیستم دوم بسته ای را که flag های SYN و ACK در آن تنظیم شده است به سیستم اول پاسخ می دهد. (آمادگی برای ارتباط)

**مرحله سوم:** در این مرحله سیستم اول پاسخی را به سیستم دوم ارسال می کند که فقط حاوی ACK flag درون بسته ارسالی می باشد. (برقراری ارتباط)

اگر سه مرحله بالا بدون هیچ مشکلی انجام شود، یک ارتباط TCP بین دو سیستم برقرار شده است.

### • آشنایی با flag های TCP

در ساختار TCP شما به موردی به نام Flag بر خواهید خورد. Flag به معنی پرچم می باشد. زمانی که مانند تصویر بالا ارتباطی آغاز می گردد، به بسته به سمت مقصد ارسال می شود که نشانگر درخواست برقراری ارتباط است. این بسته حاوی بخشی به نام Flag است که اگر قسمت SYN در آن برابر یک باشد، به معنی درخواست آغاز ارتباط می باشد. لیست Flag ها و کاربرد آن به صورت زیر است.

SYN(Synchronize) : از این flag برای آغاز یک ارتباط بین دو سیستم استفاده می شود.

ACK(Acknowledgment) : از این flag به منظور تصدیق رسیدن یک بسته استفاده می شود.

PSH(Push) : این flag به منظور ارسال بافاصله داده های بافر شده استفاده می شود.

RST(Reset) : از این flag به منظور دوباره راه اندازی ارتباط استفاده می شود.

FIN(Finish) : این flag اشاره دارد به این موضوع که دیگر انتقال انجام نپذیرد.

URG(Urgent) : وجود این flag به این موضوع اشاره دارد که داده های داخل بسته باید بافاصله پردازش شوند

### three way handshake



## • UDP(User Datagram Protocol)

این پروتکل یک پروتکل بدون اتصال (connection less) می باشد یعنی برای ارسال اطلاعات ابتدا ارتباط برقرار نمی شود سپس اطلاعات ارسال شود. از این پروتکل زمانی استفاده می شود که صحت داده ها در سمت دریافت کننده مهم نبوده و سرعت از اهمیت بیشتری برخوردار باشد

امینت در این پروتکل کمتر از TCP می باشد ولی سرعت آن بیشتر است.

## • پورت

مورد دیگری که در ساختار لایه انتقال اهمیت دارد پورت یا درگاه است. پورت برای برقراری ارتباط بین کلاینت و سرور از اهمیت بسزایی برخوردار است. پورت ها به دو دسته سخت افزاری و نرم افزاری تقسیم بندی می شوند.

پورت های سخت افزاری شامل پورت VGA, Serial, 3PS, USB و از این دست می باشد. به طور کلی پورت های سخت افزاری به صورت فیزیکی قابل رویت بوده و تعداد آن ها محدود می باشد

پورت های نرم افزاری یا مجازی بر خلاف پورت های سخت افزاری قابل مشاهده نیستند و تعداد آن ها از یک تا ۶۵۵۳۵ می باشد. البته این تعداد هم برای TCP و هم برای UDP می باشد. این پورت ها به سه دسته تقسیم بندی می شوند.

۱۰۲۴-۱ پورت های مربوط به سرویس های خاص شبکه که به آن ها پورت های ثبت شده نیز گفته می شود.

۴۹۱۵۱-۱۰۲۵ پورت های تصادفی یا رندوم نامیده می شوند و زمانی که قصد برقراری ارتباط به طور مثال وب در شبکه را داریم. پورتهای که در مقصد باز می شود ۸۱ بوده و پورت باز شده سمت ما از این دسته می باشد.

۶۵۵۳۵-۴۹۱۵۱ این پورت ها که آزاد نامیده می شوند، بیشتر در برنامه نویسی کاربرد دارند

نکته ای قابل توجه این است که در زمان برقراری ارتباط بین کلاینت و سرور می بایست پورت مورد نظر در سرور باز بوده و در سمت کلاینت نیز پورت مورد نظر قابل دسترسی باشد. حال چگونگی مدیریت ترافیک ورودی و خروجی و همچنین مدیریت ساختار پورت ها بر عهده سیستمی تحت عنوان فایروال یا دیواره آتش است

## • پروتکل های لایه کاربرد

## HTTP(hyper text transfer protocol)

پروتکلی است که سرویس دهنده و سرویس گیرنده وب از آن برای تبادل پیغام ها و همچنین دیدن صفحات وب در سمت سرویس گیرنده استفاده می کنند. زمانی که شما یک صفحه وب را مشاهده می کنید، در واقع از این پروتکل استفاده کرده اید. پورت مربوط به آن ۸۰ است.

## • HTTPS

یک پروتکل مطمئن برای تبادل اطلاعات در وب می باشد که S پایان آن نشان دهنده SSL بوده که برای انجام سرویس های احراز هویت و رمزنگاری استفاده می شود. پورت مربوط به آن ۴۴۳ است.



### • FTP(file transfer protocol)

پروتکلی است به منظور ارسال و دریافت فایل بین سیستم های TCP/IP استفاده می شود. پورت مربوط به آن ۲۰ است

### • TFTP

این پروتکل نسخه کوچک شده FTP بوده که برای انتقال فایل در شبکه به کار گرفته می شود. اما به جای TCP از UDP استفاده می کند. پورت مربوط به آن ۶۹ است

### • SMTP(simple mail trasport protocol)

از این پروتکل سرورهای نامه های الکترونیکی برای انتقال پیام به یکدیگر استفاده می کنند. پورت مربوط به آن ۲۵ است.

### • POP3(post office protocol)

پروتکلی است که سرویس گیرنده های ایمیل از آن برای دریافت ایمیل از یک سرور استفاده می کنند. پورت مربوط به آن ۱۱۰ است.

### • NTP(network time protocol)

پروتکلی است که کامپیوترهای روی یک شبکه را قادر می سازد با تبادل سیگنال های زمانی، ساعت خود را با کامپیوترهای دیگر همزمان کنند. پورت مربوط به آن ۱۲۳ است.

### • DNS(domain name system)

سیستم های TCP/IP از این پروتکل برای تحلیل نام میزبان ها به آدرس IP مورد نیاز برای تبادل اطلاعات استفاده می کنند. پورت مربوط به آن ۵۳ است.

### • DHCP(dynamic host configuration protocol)

از این پروتکل برای دادن IP به صورت اتوماتیک استفاده می شود. پورت مربوط به آن ۶۸ و ۶۷ است.

### • SNMP(simple network management protocol)

یک پروتکل مدیریتی شبکه است که مدیران شبکه از آن برای جمع آوری اطلاعات از اجزای شبکه استفاده می کنند مانند مدیریت روترها که پورت مربوط به آن ۱۶۱ است.

### • TELNET

پروتکلی است که کاربر را قادر می سازد تا به کامپیوتر از راه دور وصل شد و دستورات خود را در آن اجرا کند. پورت مربوط به آن ۲۳ است  
 نکته: لازم به ذکر است که در هر ارتباط یک سمت کلاینت بوده و طرف دیگر سرور می باشد و تمامی پورت هایی که برای موارد فوق بیان گردید، مربوط به سرور می باشد و در کلاینت پورت رندوم باز خواهد شد

## ❖ معماری شبکه

معماری یک شبکه بیانگر استانداردهای تعریف شده در خصوص نحوه اتصال کامپیوترها با یکدیگر و نحوه ارسال اطلاعات میباشد. به عبارت دیگر معماری شبکه مجموعه‌ای از استانداردهایی است که نوع کابل کشی، اتصالات، توپولوژی، نحوه دسترسی به خطوط انتقال و سرعت انتقال را مشخص می‌کند. بنابراین هنگام راه‌اندازی یک شبکه، باید ابتدا معماری شبکه مشخص شود و سپس با توجه به استانداردهایی که معماری شبکه مشخص می‌کند، قطعات و اتصالات شبکه خریداری و پیکربندی گردد.

• انواع معماری شبکه:

✓ اترنت (Ethernet)

✓ Token Ring

✓ FDDI

✓ Wireless

اترنت:

اترنت متداولترین معماری شبکه است که با استفاده از مجموعه‌ای از قوانین و استانداردها، پیکربندی بستر شبکه و بالطبع نقل و انتقال داده‌ها در شبکه را قانونمند می‌کند. به عبارت دیگر با ارائه یکسری از استانداردها و یکسری محدودیتها در بکارگیری تجهیزات، اتصالات، پهنای باند و ... تمام اجزای شبکه را با هم همزمان می‌کند.

مفهوم پهنای باند (Band Width) :

در سیستم‌های انتقال آنالوگ پهنای باند به حد فاصل بین پایین‌ترین و بالاترین فرکانسی که یک رسانه میتواند از خود عبور دهد گفته می‌شود پهنای باند بر حسب فرکانس و با واحد هرتز بیان می‌شود **300hz - 3000hz**

در سیستم‌های انتقال دیجیتال پهنای باند به ظرفیت انتقال اطلاعات گفته می‌شود و با واحد **bps** (بیت در ثانیه) سنجیده می‌شود (در مودم ۱۵ bps به معنی ۵۶۰۰ بیت در ثانیه انتقال میابد)

از عوامل موثر در پهنای باند طول، قطر و جنس کابل است. پهنای باند با طول کابل نسبت معکوس و با قطر کابل نسبت مستقیم دارد. یعنی هرچه طول کابل بیشتر شود پهنای باند کمتر شود و هر چه قطر کابل بیشتر شود پهنای باند نیز بیشتر است.

برای انتقال اطلاعات میتوان به دوروش از پهنای باند استفاده کرد:

تک باند (BaseBand)

پهن باند (Band Broad)

در روش Base Band از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می‌شود. به این معنی که در روش تک باند رسانه در هر لحظه فقط میتواند یک سیگنال را از خود عبور دهد در نتیجه ارسال نوبتی می‌شود و اطلاعات پشت سر هم و به صورت سریال ارسال می‌شوند. این روش انتقال دلیل بوجود آمدن مفهوم بسته (Pachet) است. در شبکه‌های محلی از این روش برای انتقال اطلاعات استفاده می‌شوند بدین ترتیب که از دو رشته کابل استفاده می‌شود که یکی برای ارسال و دیگری دریافت اطلاعات را انجام می‌دهد. اطلاعات بصورت بسته‌های



مشخص پشت سر هم قرار میگیرند و ارسال شده و دریافت میگردد، تمام سیستمهای انتقال دیجیتال از روش Base Band استفاده می کنند (کابل هم محور UTP)

در روش پهن باند (Band Broad): یک رسانه (کابل) میتواند در آن واحد یک یا چند سیگنال را به طور همزمان عبور دهد. هر سیگنال به صورت جداگانه ارسال می شود و تداخل بین سیگنالهایی متفاوت به وجود نمیاید. از این روش در سیستمهای انتقال آنالوگ استفاده می شود و رسانه میتواند در آن واحد سیگنالهای متفاوتی را با فرکانسهای مختلف از خود عبور دهد. از این روش در شبکه تلویزیونهای کابلی و شبکه های WAN استفاده میگردد (کابل هم محور - فیبرنوری)

### سرعت انتقال اطلاعات :

مقدار اطلاعاتی که در واحد زمان توسط تجهیزات شبکه ارسال می شود گفته می شود مثال کارت شبکه 100mbps

سرعت انتقال اطلاعات با پهنای باند رابطه مستقیم دارد. هر چه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می شود و بر عکس.

نکته : پهنای باند، ظرفیت انتقال یک رسانه یا یک کابل است. در صورتی که سرعت انتقال، سرعت ارسال اطلاعات در واحد زمان است.

### TOKEN RING

شبکه TOKEN RING از نظر ظاهری یک شبکه ستاره ای است ولی به صورت TOKEN PASSING کار می کند. در این شبکه یک حلقه منطقی به وجود میاید و TOKEN در امتداد حلقه حرکت کرده و به کامپیوترها میرسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد TOKEN را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می کند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت TOKEN مسیر خود را طی می کند تا به کامپیوتر مقصد برسد. کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی. در جواب یک بسته به نام ACKNOWLEDGE به کامپیوتر مبداء ارسال می کند. کامپیوتر مبداء نیز TOKEN اصلی را از بین برده و یک TOKEN جدید تولید مینماید و آنرا در امتداد مسیر TOKEN قبلی به حرکت در می آورد. این پروسه به همین صورت ادامه خواهد یافت.

در شبکه TOKEN RING در محل اتصال کامپیوترها به جای هاب از دستگاهی بنام MAU استفاده می شود. سرعت انتقال اطلاعات در این شبکه 16 MBPS یا 4 MBPS است. کارتهای 16 MBPS میتوانند با سرعت 4 MBPS نیز فعالیت کنند.

در شبکه TOKEN RING از کابل های زوج به هم تابیده استفاده می شود. اگر از کابل UTP در این توپولوژی استفاده شود. حداکثر طول کابل میتواند ۴۵۲۳ متر باشد و این شبکه فقط با سرعت ۲ مگابیت در ثانیه کار می کند و اگر از کابل STP استفاده شود. حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابیت در ثانیه اطلاعات منتقل می شود.

### FDDI

FDDI، تکنولوژی یک شبکه با سرعت ۱۰۰ مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده می کند. در این تکنولوژی به جای فیبر نوری از کابل مسی نیز میتوان استفاده کرد ولی در صورت استفاده از کابل مسی طول کابل کمتر می شود. FDDI به عنوان BACKBONE در محلهایی که تعداد زیادی کامپیوتر در آن قرار دارد، استفاده می شود. از جمله این محیطها میتوان به دانشگاهها اشاره کرد. در FDDI میتوان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتر به یکدیگر متصل کرد. توپولوژی فیزیکی این شبکه حلقوی است. نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر ساخته می شود و در هر ۲ کیلومتر یک تقویت کننده قرار میگیرد.

برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود میآید ، از دو حلقه فیبر نوری در کنار هم استفاده می شود تا در صورتی که یکی از رشته ها قطع شود ، رشته دوم وارد عمل شده و جایگزین رشته اول شود.

### ✓ شبکه بدون سیم Wireless

شبکه بدون سیم، شبکه ای است که از امواج رادیویی BROAD BAND برای مرتبط کردن کامپیوترها به یکدیگر استفاده می کند. از سیستم بیسیم در شبکه های WAN استفاده می شود. کاربرد آن می تواند مرتبط کردن دو یا چند شبکه محلی ، ارائه سرویس اینترنت و سرویسهای دیگر باشد. شبکه بیسیم برای برقراری بین کامپیوترهایی که نزدیک یکدیگر قرار دارند نیز استفاده می شود که در این صورت نوعی شبکه به نام PAN بکار میرود.

در شبکه های PAN نیازی به استفاده از تجهیزات خاص شبکه نیست و فقط با نصب دو کارت شبکه PAN روی دو کامپیوتر که در فاصله مناسب از یکدیگر قرار گرفته اند می توان یک شبکه را راه اندازی کرد. از مزایای شبکه بیسیم اینست که نیازی به نصب کابل شبکه و تجهیزات آن نیست و سرعت انتقال اطلاعات نیز می تواند تا سرعت ۳۳ مگابیت در ثانیه افزایش پیدا کند.

### ❖ Performance & Fault Tolerance

برای نگهداری شبکه و پایداری استفاده از آن، باید مواردی از جمله سرعت، نحوه خدمات دهی و همچنین پیش بینی شرایط بحران را در نظر گرفت.

در این قسمت ما به دو بخش RAID و Backup اشاره خواهیم کرد.

قبل از شروع مبحث RAID لازم است مطالبی را در مورد مدیریت هارد و اصطلاحات آن را بیان کنم.

#### • مدیریت هارد دیسک

تقسیم بندی های مختلفی برای انواع هارد و مدیریت آن ها وجود دارد، که یکی از آن ها MBR یا GPT بودن آن است که به آن اشاره می شود یکی از مشکلات قدیمی در مدیریت دیسک ها عدم پشتیبانی از درایوهای بیش از ۳۲ گیگابایت بود که با ساختار فایل FAT ۳۲ سازگار نبود و مدیر سیستم می بایست ساختار فایل درایو را به NTFS تغییر دهد. همین مشکل برای درایوهایی با بیش از دو ترابایت بر روی ویندوز سرور ۲۰۰۳ نیز مشاهده شده است. به صورت پیش فرض ۲۰۰۳ Windows Server از درایوهایی با بیش از TB2 پشتیبانی نمی نماید. البته مشکل فوق حتی با فایل سیستم NTFS نیز قابل حل نخواهد بود. حال برای رفع مشکل فوق بایستی محل ذخیره سازی اطلاعات مربوط به فایل سیستم دیسک تعریف شده در ویندوز را از MBR به GPT تغییر دهیم.

با انجام این کار می بینیم که سیستم عامل فضایی بیشتر از TB ۲ را پشتیبانی می نماید. فضایی در حدود ۲۵۶ ترابایت برای تغییر نوع دیسک خود از MBR به GPT کافیت در قسمت خط فرمان خود دستور DISKMGMT.MSC را تایپ نموده و در کنسول مدیریت دیسک بر روی دیسک مورد نظر تان راست کلیک کرده و گزینه CONVERT TO GPT DISK را انتخاب کنید.

نوع دیگر تقسیم بندی از لحاظ Basic یا Dynamic بودن هارد است. هارد های از نوع Basic به منظور نصب ویندوز مناسب می باشند. هارد از نوع Dynamic به منظور استفاده در RAID به کار می رود.

نکته حائز اهمیت این است که تبدیل این دو به همدیگر امکان پذیر می باشد. فقط در هنگام تبدیل از Basic به Dynamic، اطلاعات از بین نرفته ولی به صورت بالعکس اطلاعات شما از بین می رود.

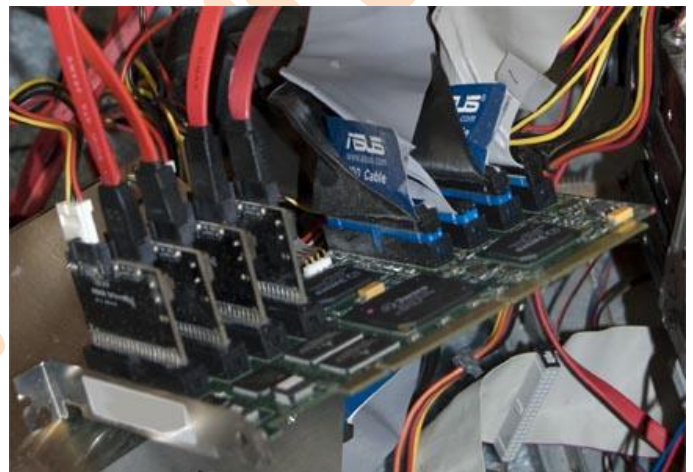
نکته دیگر که باید در نظر داشت این است که هیچ گاه هاردی که در آن ویندوز نصب شده است را به Dynamic تبدیل نکنید.

#### • RAID

یکی از مفاهیم مهمی که در این قسمت باید به آن توجه نمود، RAID (Redundant Array of Independent Disks) می باشد

RAID هم به صورت سخت افزاری و هم به صورت نرم افزاری قابل پیاده سازی می باشد. در زیر نمونه هایی از سخت افزارهای

RAID را مشاهده می کنید که در آن چندین Slot برای قرار دادن هارد وجود دارد.



RAID یکی از موارد افزایش تحمل خطای سیستم است. روشهای مختلفی برای ترکیب چند هارد دیسک در یک آرایه، بسته به نیاز برنامه های کاربردی، وجود دارد. اما در همه حالات استفاده از چندین درایو نتایجی چون: افزایش گنجایش، امنیت داده و کارایی درایوها را به دنبال خواهد داشت. به یاد داشته باشید که این روشها روشهای خیلی ارزانی نیستند و همیشه با پیچیدگی و هزینه های زیادی همراهند.

از زمان اختراع کامپیوتر تا به حال کدهای نرم افزاری رشد زیادی داشته اند. و این رشد نیاز به یک محیط ذخیره سازی بزرگ را افزایش داده است و ابداع شبکه های محلی و اینترنت نیز این نیاز را شدیدتر کرده است. مبنای کار RAID فضای دیسک است و توانسته است با ترکیب فضای هاردهای کوچک با هم در یک مخزن بسیار بزرگ مشکلات را برطرف کند. پیش از این RAID به دلیل هزینه های بسیار بالای سخت افزار مورد نیاز آن، بیشتر برای کاربردهای تجاری با حوزه های محدود به کار میرفت. ولی در چند سالها اخیر این امر دچار تغییر شده است، از میان تمام سروصدهایی که برای بهبود کارایی و استفاده بهتر از زمان می شود، RAID توانسته راه خود را باز کند و یک پله بالاتر از همه قرار بگیرد. افزایش کنترلرهای RAID ارزان که میتواند با نسخه ی مصرف کننده ی IDE/ATA کار کنند مانند آنچه واحدهای گرانقیمت SCSI انجام می دهند اشتیاق همگان را به RAID افزایش داده است. و این گرایش شاید ادامه یابد. در حال حاضر نیز تعداد زیادی از سازندگان مادربرد، بوردهای خود را با حمایت از استاندارد RAID به بازار عرضه می کنند. متأسفانه RAID در زمینه ی کامپیوتر به طور واقعی اشکالات را برطرف نمی کند. با این حال اگر به طور صحیح اجرا شود، میتواند زمان از کارافتادگی را از بین ببرد.

## • انواع RAID ها

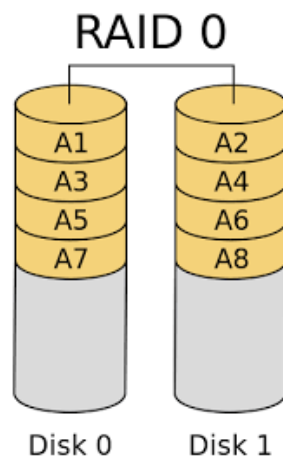
RAID ها انواع مختلفی را شامل می شوند که از مهمترین و پرکاربردترین آن ها RAID صفر، RAID یک و RAID پنج می باشد که به آن ها اشاره خواهیم کرد.

## ✓ RAID صفر

این نوع از RAID شامل مجموعه دیسکهای جدا که در آن اطلاعات به صورت بالک بالک روی هر دو دیسک ذخیره می شوند. کارایی بهتر و افزودنی ذخیره سازی را فراهم می کند اما بدون توانایی تحمل نقص و اشکال می باشند. خرابی هر یک از هاردیسکها باعث از بین رفتن آرایش می شود. خرابی یک هاردیسک نابودی کل آرایش را به همراه دارد، زیرا اطلاعاتی که در این مدل نوشته می شود اطلاعات به قطعاتی شکسته می شود. تعداد قطعات توسط تعداد هاردیسکها مشخص می شود. قطعات اطلاعات با هم در سکتورهای مشابه در دیسکهای مربوطه نوشته می شود.

این اجازه می دهد قطعات کوچکتر از کل قطعه بزرگ بطور موازی از درایوها خوانده شود که نتیجه این مدل چینه پهنای باند زیاد می باشد. هنگامی که یک سکتور روی یکی از دیسکها خراب شود سکتورهای مشابه روی تمام دیسکهای دیگر بدون استفاده خواهد بود. زیرا بخشی از اطلاعات خراب شده است. این مدل چینه بررسی خطا ندارد بنابر این هر خطایی غیرقابل بازبانی خواهد بود. دیسکهای بیشتر پهنای باند بیشتری را در پی خواهد داشت اما ریسک از دست دادن اطلاعات نیز بیشتر می شود.

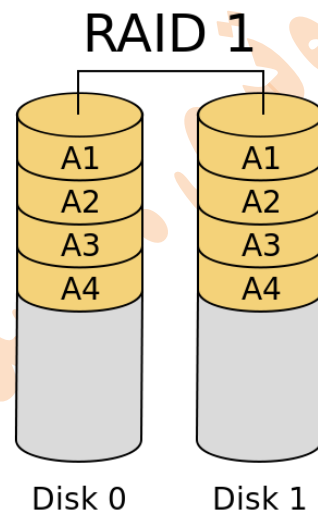
RAID صفر سریعترین و مناسبترین روش از میان تمامی حالات RAID است. و بهترین کارمفید و کارایی را در ذخیره سازی داده ها ارائه می دهد. ولی باید گفت که هیچگونه تحمل خطایی ندارد. اگر یکی از دیسکها دچار مشکل شود، تمام آرایه از کار می افتد و هیچ راهی برای بازگرداندن داده های از دست رفته وجود ندارد. در RAID ۰، کارایی به اندازه ی بلوکها بستگی دارد. اگر اندازه ی آن ها خیلی کوچک باشد دستورات برای اجرا در عملیات نوشتن متمرکز می شوند، علاوه بر آن به دستورات واسط سخت افزاری بیشتری نیاز است. بهینه سازی اندازه ی بلوکها باعث می شود که افزایش توان عملیاتی کار می شود، به ویژه برای درخواستهای موازی برای خواندن داده ها. اندازه ی بلوکها قابل تنظیم است. ولی شما باید بیت به بیت آزمایش کنید تا به نتیجه ی مطلوب برسید. اما یکی از نقاط شروع خوب برای حداقل اندازه ی بلوک ۱۶ کیلوبایت است. برای محیطهای چندکاربره میتوانیم آرایه را با نوارهای بزرگ تنظیم کنیم. برای سیستمهای تک کاربره که به طور مداوم با رکوردها سروکار دارند نیز میتوان اندازه ی نوارهای موجود در آرایه را کوچک تر در نظر گرفت. به طور نمونه اندازه ی فایل ۴۸ کیلوبایت است. ۱۶ کیلوبایت از این فایل روی دیسک اول، ۱۶ کیلوبایت در دیسک دوم و ۱۶ کیلوبایت دیگر در دیسک سوم نوشته می شود.



## RAID 1 ✓

به این سطح ، mirroring نیز گفته می شود و اساساً یک ترکیب از دو هارد دیسک است که اطلاعات یکی از این دو ، عیناً روی دیگری کپی می شود و در کامپیوتر به صورت یک درایو نمایش داده می شود. تحمل خطا در RAID ۱ وجود دارد. چراکه اگر یکی از دیسکها از کار بیفتد آرایه میتواند همچنان به فعالیت خود ادامه دهد. به دلیل اینکه همزمان از دو هارد دیسک استفاده می شود ، زمان خواندن سریعتر می شود. روشی که در اینجا برای خواندن دادهها به کار گرفته می شود ، زمانبندی ( Round-robin ) روح سرگردان نام دارد. که سرور برای خواندن داده ها مرتباً از یک هارد به هارد دیگر می رود و عملاً زمان را بین دو هارد دیسک تقسیم می کند.

سرعت خواندن در این جا دوبرابر سرعت خواندن از یک درایو منفرد فاقد mirroring است. با این حال در موقع نوشتن ، دادهها باید روی دو هارد دیسک نوشته شوند. و عملاً میبینیم که در مدت زمان نوشتن تغییری حاصل نخواهد شد. نسبت به سایر انواع آرایه های افزایشی ، این سطح بهترین کارایی را دارد. ولی از لحاظ رتبه در هنگام از کار افتادن درایو ، نسبت به RAID5 کارایی کمتری دارد. بزرگترین عیب این سطح هزینه ای است که برای درایوهای اضافی آن پرداخت می شود. به هر حال هیچ چیز ارزان به دست نیاید و برای داشتن یک سیستم امن و کارآ باید هزینه های زیادی پرداخت چراکه اگر سیستم از کار بیفتد یا حتی برای ساعتی متوقف شود ، هیچ هزینه ای نمیتواند جایگزین دادهها و اطلاعات باارزش از دست رفته ما باشد.

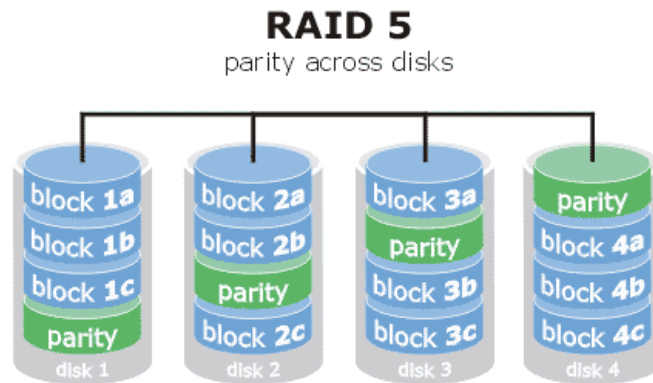


## RAID5 ✓

اساساً RAID ۵ شبیه RAID ۱ است. با این تفاوت که RAID ۵ برای هر نوار از دادهها یک پربیتی ذخیره می کند. اما در مقایسه با RAID ۱ عملیات نوشتن آهسته تر است. زیرا یک زمان اضافی برای نوشتن اطلاعات پربیتی نیاز است. در موقع نوشتن اطلاعات RAID ۵ تقریباً ۶۰ درصد آهسته تر از RAID ۱ عمل می کند. عملیات خواندن هم هیچ تغییری پیدا نمی کند. برای رسیدن به بهترین کارایی ، RAID ۵ باید یک فضای ذخیره سازی داشته باشد برابر با حاصل جمع فضای تمامی هاردها منهای ۱. بعضی مواقع به این سطح از RAID ، “آرایه با پربیتی چرخشی” نیز گفته می شود. چرا که مانند RAID ۴ پربیتی ها را در یک درایو جداگانه جمع نمی کند و این اطلاعات را در تمام آرایه با تمام درایوها توزیع می کند. هیچ درایو منحصر بفردی برای ذخیره ی اطلاعات پربیتی وجود ندارد. تمام درایوها شامل داده هستند و عملیات خواندن میتواند از تمام درایوها به صورت مشترک انجام شود. برای نوشتن اطلاعات نیز به یک درایو داده و نیز یک درایو دیگر برای ذخیره ی اطلاعات پربیتی نیاز داریم. با توجه به اینکه ، پربیتی رکوردهای مختلف روی درایوهای دیگر قرار میگیرد ، عملیات نوشتن معمولاً میتواند به اشتراک گذاشته شود



بیشترین استفاده از RAID ۵ در سرورها و شبکه‌های محلی می‌باشد، جایی که فضای ذخیره سازی و تحمل خطا بسیار اهمیت دارد. در این روش نیازی به وجود درایو آینه وجود ندارد. زیرا اگر یکی از دیسک‌های اصلی از کار بیفتد، سرور اطلاعات از دست رفته از نوارهای پریته ذخیره شده روی دیگر درایوها بازسازی می‌کند. برای اجرای RAID ۵، حداقل به سه هارد دیسک نیاز داریم.



#### • سخت‌افزارهای شبکه

✓ کارت شبکه

کارت شبکه، آداپتور شبکه یا کارت واسط شبکه Network Interface Card قطعه‌ای از سخت‌افزار رایانه است و طراحی شده تا این امکان را به رایانه‌ها بدهد که بتوانند بر روی یک شبکه رایانه‌ای با یکدیگر ارتباط برقرار کنند. این قطعه دسترسی فیزیکی به یک رسانه شبکه را تأمین می‌کند و با استفاده از آدرس‌های MAC در شبکه کار می‌کند. این شرایط به کاربران اجازه می‌دهد تا به وسیله کابل یا به صورت بی‌سیم به یکدیگر متصل شوند.



## Repeater ✓

تکرارگر تجهیز الکترونیکی است که سیگنالی را دریافت کرده و آن را با سطح دامنه بالاتر، انرژی بیشتر و یا به سمت دیگر یک مانع ارسال می کند. بدین ترتیب می توان سیگنال را بدون کاستی به فواصل دورتری فرستاد. از آنجا که تکرارگرها با سیگنال های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده ای که انتقال می دهند تلاشی نمی کنند، این تجهیزات در «لایه فیزیکی» یعنی اولین لایه از مدل مرجع OSI عمل می کنند.



## Hub ✓

هاب قطعه ای سخت افزاری است که امکان اتصال قسمت های یک شبکه را با هدایت ترافیک در سراسر شبکه فراهم می کند. هاب ها در (لایه فیزیکی) از مدل مرجع OSI عمل می کنند. عملکرد هاب بسیار ابتدایی است، به این ترتیب که داده رسیده از یک گره را برای تمامی گره های شبکه کپی می کند. هاب ها عموماً برای متصل کردن بخش های یک (شبکه محلی) بکار می روند. هر هاب چندین پورت یا همان درگاه دارد. زمانی که بسته ای از یک درگاه می رسد، به دیگر درگاه ها کپی می شود، بنابراین همه قسمت های شبکه محلی می توانند بسته ها را ببینند.



## Bridge ✓

یک پل دو زیرشبکه (سگمنت) را در لایه پیوند داده از مدل مرجع OSI به هم متصل می کند. پل ها شبیه به تکرارگرها و هاب های شبکه اند که برای اتصال قسمت های شبکه در لایه فیزیکی عمل می کنند، با این حال پل با استفاده از مفهوم پل زدن کار می کند، یعنی به جای آنکه ترافیک هر شبکه بدون نظارت به دیگر درگاه ها کپی شود، آنرا مدیریت می کند.



پل‌ها به سه دسته تقسیم می‌شوند:

پل‌های محلی: مستقیماً به شبکه‌های محلی متصل می‌شود.

پل‌های دوردست: از آن می‌توان برای ساختن شبکه‌های گسترده جهت ایجاد ارتباط بین شبکه‌های محلی استفاده کرد. پل‌های دوردست در شرایطی که سرعت اتصال از شبکه‌های انتهایی کمتر است با مسیریاب‌ها جایگزین می‌شوند.

پل‌های بی‌سیم: برای اتصال شبکه‌های محلی به شبکه‌های محلی بی‌سیم یا شبکه‌های محلی بی‌سیم به هم یا ایستگاه‌های دوردست به شبکه‌های محلی استفاده می‌شوند.

Switch ✓

راهگزین که بیشتر واژه سوئیچ برای آن بکار برده می‌شود، وسیله‌ای است که قسمت‌های شبکه را به یکدیگر متصل می‌کند. راهگزین‌های معمولی شبکه تقریباً ظاهری شبیه به هاب دارند، ولی یک راهگزین در مقایسه با هاب از هوشمندی بیشتری و همچنین قیمت بیشتری برخوردار است. راهگزین‌های شبکه این توانمندی را دارند که محتویات بسته‌های داده‌ای که دریافت می‌کنند را بررسی کرده، دستگاه فرستنده و گیرنده بسته را شناسایی کنند، و سپس آن بسته را به شکلی مناسب ارسال نمایند. با ارسال هر پیام فقط به دستگاه متصلی که پیام به هدف آن ارسال شده، راهگزین پهنای باند شبکه را به شکل بهینه تری استفاده می‌کند و عموماً عملکرد بهتری نسبت به یک هاب دارد. از نظر فنی می‌توان گفت که راهگزین در لایه پیوند داده از مدل مرجع OSI عمل کنند. ولی بعضی انواع راهگزین قادرند تا در لایه‌های بالاتر مانند لایه سه نیز به بررسی محتویات بسته بپردازند و از اطلاعات بدست آمده برای تعیین مسیر مناسب ارسال بسته استفاده کنند.



Router ✓

مسیریاب‌ها تجهیزات شبکه‌ای هستند که بسته‌های داده را با استفاده از سرایندها و جدول ارسال تعیین مسیر کرده، و ارسال می‌کنند. مسیریاب‌ها در لایه شبکه از مدل مرجع OSI عمل می‌کنند. همچنین مسیریاب‌ها اتصال بین بسترهای فیزیکی متفاوت را امکان پذیر می‌کنند. این کار با چک کردن سرایندها یک بسته داده انجام می‌شود. هر مسیریاب دسته کم به دو شبکه، معمولاً شبکه‌های محلی، شبکه‌های گسترده و یا یک شبکه محلی و یک سرویس‌دهنده اینترنت متصل است.



### Access point ✓

دستگاهی است برای برقرای ارتباط بین دستگاه‌های بدون سیم به یکدیگر با هدف تشکیل یک شبکه بدون سیم و در اغلب موارد نقش پل ارتباطی بین این شبکه بدون سیم را با یک شبکه اینترنت سیمی نیز بر عهده دارد.

access point ها همچون یک مرکز فرستنده و گیرنده امواج رادیویی شبکه‌های بدون سیم عمل می‌کنند.

وقتی در یک شبکه بدون سیم از access point استفاده می‌کنیم، این شبکه در اصطلاح در مد Infrastructure عمل می‌کند در غیر اینصورت و عدم استفاده از access point در شبکه بدون سیم در مد 'ad hoc' یا 'peer to peer' می‌باشد.



### WAN Link ✓

WAN Link تکنولوژی ای است که به عنوان یک زبان مشترک، ارتباط بین دو منطقه مختلف را برقرار می‌نماید.

### انواع WAN Link

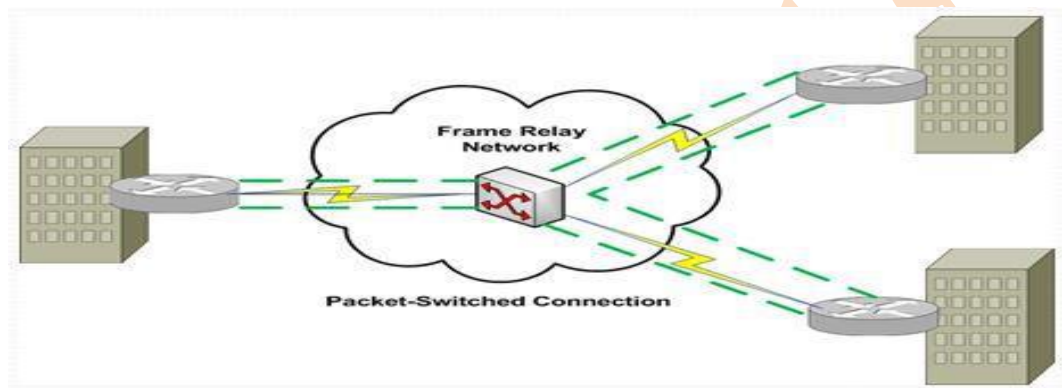
- FRAME RELAY
- ATM
- ISDN
- PSTN
- Leased Line

- SoNet/oc-x
- DSL
- ADSL
- SDSL

#### : FRAME RELAY

یک نوع بستری برای ارتباط بین شهرهای بزرگ و کشورها می باشد. FRAME RELAY را تعدادی سوئیچ و روتر به صورت ابری تشکیل می دهند. FRAME RELAY دارای پروتکل و ساختار مخصوص به خود می باشد.

در این بستر مقدار انتقال داده و نحوه انتقال آن تنظیم می گردد. بستر این تکنولوژی اینترنت نیست به همین دلیل از امنیت بالایی برخوردار است ولی می تواند از اینترنت استفاده کند. معمولاً دولت ها آن را راه اندازی می کنند.



#### ATM(asynchronous transfer mode)

ATM یک استاندارد برای شبکه های سریع است که یک قالب برای ایجاد شبکه های سریع با استفاده از پروتکل های مخابراتی سریع و متنوع به عنوان پروتکل لایه فیزیکی ارائه می کند. این قالب بسیار انعطاف پذیر و قوی بوده و قابلیت ارائه سرویسهای متنوعی از لحاظ کیفیت سرویس را دارا می باشد ( این قالب مبتنی بر ارسال اطلاعات بصورت سلولهای بسیار کوچک اطلاعاتی ) بستههای کوچک با ابعاد ثابت بر روی مسیرهای داده های اتصال گرا Connection Oriented می باشد . بستر آن فیبر نوری است و تا 622 mb/s سرعت آن ارتقا پیدا می کند و بیشتر برای ارسال تصویر و فیلم در خبرگزاری ها کاربرد دارد.

#### Intergeated Service Digital Network (ISDN )

اساس یک شبکه کاملاً دیجیتال پی ریزی شده است. در حقیقت تلاشی برای جایگزینی سیستم تلفنی آنالوگ با دیجیتال بود که علاوه بر داده های صوتی، داده های دیجیتال را به خوبی پشتیبانی کند. به این معنی که انتقال صوت در این نوع شبکه ها به صورت دیجیتال می باشد. در این سیستم صوت ابتدا به داده های دیجیتال تبدیل شده و سپس انتقال می یابد . سرعت بالاتری را برای انتقال فراهم می آورد می تواند یک صدای دیجیتال واضح کریستالی را برایتان فراهم نماید حتی اگر خطوط شما آنالوگ باشد یک خط ISDN می تواند دو خط تلفن دو شماره تلفن و یک خط سومی را جهت پیوند ارتباط داده های در بر داشته باشد.

ISDN به دو شاخه اصلی تقسیم می شود: B-ISDN و N-ISDN

## B-ISDN: Broadband ISDN

شبکه‌ای با پهنای باند بالا برای انتقال داده می‌باشد.

## N-ISDN: Narrowband ISDN

با پهنای باند پایین است که برای استفاده‌های شخصی طراحی شده‌است.

## PSTN(public switched telephone network)

ساده ترین تکنولوژی wan می‌باشد که در خطوط تلفن به کار می‌رود و خطوط آنالوگ می‌باشد.

پهنای باند آن  $33.6 \text{ kb/s}$  می‌باشد

Leased line : خطوط اجاره‌ای می‌باشند. دارای استاندارد های زیر هستند.

T1 که ارزانتر از استاندارد های دیگر است و سرعت انتقال آن  $1.544 \text{ mb/s}$  است. که این استاندارد خود به 24 کانال تقسیم می‌شود..

T3 که سرعت انتقال آن  $44.736 \text{ mb/s}$  می‌باشد و خود به ۶۷۲ کانال تقسیم می‌شود.

E1 که استاندارد اروپا بوده و  $2.48 \text{ mb/s}$  سرعت انتقال آن است

E3 که استاندارد اروپا بوده و  $34.368 \text{ mb/s}$  سرعت انتقال آن است. به ۵۱۲ کانال تقسیم می‌شود

SoNet/oc-x: تکنولوژی است که بیشتر در data center ها مورد استفاده قرار می‌گیرد و جز خطوط اجاره‌ای هستند که بستر آن فیبر نوری است.

## DSL(digital subscriber line)

L واژه‌ای عمومی است که به انواع سرویس‌های ارتباطی دیجیتال که از خطوط تلفن استفاده می‌کنند اطلاق می‌گردد معروفترین DSL در ایران ADSL می‌باشد.

سرعت دانلود و آپلود آن یکسان نیست.

پهنای باند آن برای دانلود  $9 \text{ mb/s}$  و برای آپلود  $1 \text{ mb/s}$  می‌باشد

فاصله مرکزی که به ما این فناوری را انتقال می‌دهد اهمیت دارد. از اسپلیتر برای تقویت سیگنال ارتباطی و جلوگیری از نویز در ADSL استفاده می‌شود.

DSL ها انواع مختلفی دارند از جمله SDSL است که سرعت دانلود و آپلود آن  $2.3 \text{ mb/s}$  است و بیشترین پهنای باند را به می‌دهد  $13.55$  مگابیت است

## WAN Data Rates

WAN Technology	Typical Available Bandwidth
Frame Relay	56 kbps – 1.544 Mbps
T1	1.544 Mbps
T3	44.736 Mbps
E1	2.048 Mbps
E3	34.4 Mbps
ATM	155 Mbps – 622 Mbps
SONET	51.84 Mbps (OC-1) – 159.25 Gbps (OC-3072)

### ❖ دستورات کاربردی شبکه

در این قسمت برخی از دستورات مربوط به شبکه رو قرار می دهیم . دستورات مربوط به سیستم عامل ویندوز اولین دستوری که در ساختار شبکه بسیار استفاده می شود دستور ping می باشد این دستور در قسمت های قبلی توضیح داده شده است و برای تست برقراری ارتباط مورد استفاده قرار می گیرد. نحوه استفاده این دستور به صورتی است که ابتدا وارد محیط CMD شده و پس از تایپ ping آی پی سیستم مقصد را وارد می کنیم. در این حالت به صورت پیش فرض ۲ بسته ارسال و ۲ بسته دریافت خواهد شد که نشان دهنده برقراری یا عدم برقراری ارتباط است.

جهت اجرای دستور ping ابتدا در خط فرمان Dos فرمان ping را تایپ کرده و در ادامه آدرس وب سایت مورد نظرتان را وارد کنید و سپس کلید Enter را بفشارید.

**فرمان ping -t :** این فرمان سبب می شود که میزبان خاصی تا قطع شدن ارتباط دائما ping شود . از این فرمان بیشتر برای تعیین زمان قطع و وصل شدن ارتباط به شبکه می توان استفاده نمود.

**فرمان Netstat :** این فرمان در واقع یک برنامه ویژه است که به همراه سیستم عامل Windows ارائه شده است ، از این برنامه برای نمایش تمام ارتباطات موجود در شبکه و تعیین port و IP کامپیوتر هائی که در شبکه وجود دارند می توانید استفاده کنید . کافی است که بعد از اتصال به شبکه ی اینترنت این دستور را در خط فرمان Dos وارد کنید

در بخش State می توانید وضعیت پورت ها را از لحاظ Listening ، یا Established و Time - wait مشاهده کنید . در بخش Foreign Address می توانید سرور و یا کلاینتی را که با آن در ارتباط هستید و شماره port آن را مشاهده کنید . دستور Netstat دارای تعدادی سوئیچ است که در ادامه به بررسی آنها می پردازیم .

**فرمان: Netstat/ ? :** این فرمان سوئیچ های برنامه Netstat را به شما نشان می دهد درباره هر سوئیچ توضیح مختصری درباره عملکرد آن نوشته شده است.

**فرمان: Netstat -n :** همانطور که میدانید از طریق فرمان Netstat می توانیم آدرس IP و Port کامپیوتری را که در ارتباط با آن هستیم ، بدست آوریم . با تایپ فرمان Netstat -n می توان بدون استفاده از برنامه دیگری IP کامپیوتر مقابل خود را پیدا نمود . کافی است که بعد

از برقراری ارتباط از طریق اینترنت و وارد شدن به یک وب سایت این دستور را در خط فرمان Dos وارد کنید.

در ستون **port** نوع پروتکل مشخص شده است که غالبا **Tcp** می باشد. در ستون **Local Address** ،

**IP** کامپیوتر خود را مشاهده می کنید. و در ستون **Foreign Address** نیز **IP** کامپیوتری که در تماس با آن هستید به همراه پورت آن دیده می شود. در ستون **State** وضعیت ارتباط با آن کامپیوتر مشخص شده است.

**فرمان Netstat -a** : توسط این فرمان می توان تمام **Port** هائی که در یک کامپیوتر مسئول ارسال و دریافت داده ها می باشند ، مشخص نمود. کافی است که این فرمان را در خط فرمان **Dos** تایپ کرده و نتیجه را مشاهده کنید. در این حالت پورت ها با معادل اسمی خود ظاهر می شوند. بعنوان مثال پورت ۱۳۹ با معادل اسمی آن یعنی **NetBios** نشان داده می شود.

**فرمان Netstat -an** : با اجرای این فرمان می توان تمام پورت ها و **IP** ها را به صورت عددی مشاهده نمود. بعنوان مثال در یک شبکه محلی کافی است که از طریق آیکن **My Network Place** وارد یکی از پوشه ها در کامپیوتر دیگر شده و سپس این فرمان را در خط فرمان **Dos** تایپ کرده و اجرا کنید. در این حالت در ستون **Foreign Address** می توانید آدرس **IP** کامپیوتر مورد نظر را به همراه پورت آن که غالبا "۱۳۹" می باشد مشاهده کنید.

**فرمان Netstat -p XXX** : در این فرمان به جای **XXX** باید نوع پروتکل مورد نظر را انتخاب کنیم که می تواند **TCP** یا **UDP** باشد. کافی است **Netstat -p TCP** را وارد کرده و نتایج را مشاهده کنید.

**فرمان Netstat -e** : این فرمان مخصوص ویندوز ۹۸ و **ME** بوده و آمار ارتباطات و داده ها را نشان می دهد ، دستور را در خط فرمان **DOS** تایپ کرده تا نتایج را مشاهده کنید. در ویندوز **XP** با کلیک راست روی آیکن ارتباط در سمت راست نوار وظیفه و انتخاب فرمان **Status** می توانید همین نتایج را مشاهده کنید. مهمترین استفاده از این دستور دیدن **Error** ها در هنگام دریافت فایل از طریق شبکه می باشد.

**فرمان Netstat -R** : این فرمان جزئیات دقیقی مانند آدرس **Netmask** ، **Gateway** ، **Metric** و **InterFace** در اختیار شما قرار می دهد. این بخش مربوط به کاربران حرفه ای است.

**فرمان Net View** : از این فرمان برای مشاهده کامپیوترهای فعال موجود در شبکه می توان استفاده نمود ، این فرمان را در خط فرمان **DOS** تایپ کنید.

**فرمان Net Name** : از این فرمان برای پیدا کردن نام کامپیوتر می توان استفاده نمود.

**فرمان Net Send** : از این فرمان برای ارسال یک پیام فوری به یکی از کامپیوترهای موجود در شبکه می توان استفاده نمود ، پیام ارسال شده در یک کادر محاوره ای به کامپیوتر مقصد تحویل داده می شود. شکل کلی دستور به شکل زیر است:

**Net send Computer name or Ip address your message**

**دستور Finger** : به کمک این دستور شما می توانید اطلاعاتی را درباره کاربران روی کامپیوتر راه دور بدست بیاورید. برای استفاده از این فرمان ابتدا خط فرمان **Dos** را راه اندازی کرده و سپس فرمان **Finger** را تایپ نمایید.

در ادامه نام کاربری شخص را وارد کرده و سپس علامت **(@)** را وارد کنید. حال باید نام سایت مورد نظر را وارد نمایید. شکل کلی دستور به صورت زیر است **Finger Username@sitename.com**

**Ipconfig** : از این دستور برای مشاهده اطلاعات مربوط به کارت شبکه های سیستم استفاده می شود.

**Nslookup** : از این دستور به منظور مشاهده اطلاعات **DNS** استفاده می شود.

**Tracert** : این دستور به منظور مشاهده مسیر یاب های بین شما و مقصد مورد استفاده قرار می گیرد.



Netstat : اطلاعات مهمی را می توانید با استفاده از این دستور بدست آورید. از جمله این اطلاعات می توان به پورت های باز روی سیستم اشاره کرد.

### ❖ قوانین شبکه

چند قانون اصلی در شبکه وجود دارد که اعتقاد و عمل به آن اجتناب ناپذیر است

#### • کار باید شبکه Network has to work

هرچه سعی کنیم نهایتاً محدود به سرعت نور هستیم - یعنی نمی توان از ژاپن به لندن را با ۱۰ ms پینگ کرد چون فاصله فیزیکی باید توسط نور طی شود.

بسیاری از مفاهیم بصورت کامل یاد گرفته نمی شوند مگر توسط تولیدکنندگان محصولات شبکه یا کسانی که در عمل در شبکه های خود از آن تکنولوژی ها استفاده می کنند. سواد تئوری - ناقص است.

در بسیاری از موارد می توان چندین مشکل مجزا را با یک راه حل کلی رفع کرد - لزوماً این راه حل خوبی نیست.

Good, Fast و Cheap خوب - سریع - ارزان از این سه تنها میتوان دو تا را با هم داشت! همه با هم امکان پذیر نیست.

شبکه پیچیده تر از آن است که در تصور بخواهید آن را پیش بینی کنید و در نظر بگیرید

هر چه Resource و منابع داشته باشید باز هم کم است - این مورد در زمینه RAM- Storage و CPU همیشه صدق می کند. در زمینه Memory و Bandwidth هم همینطور...

یک سایز، مناسب همه نیست - یک طراحی / راه حل شبکه برای همه صدق نمی کند - اینجاست که در اکثر پاسخ ها به پرسش های شما اشاره می کنم که بستگی دارد

با زور و فشار زیاد - دستگاه ها و سرورهایی که برای آن کار در نظر گرفته نشده اند - کار خواهند کرد اما بالاخره روزی از کار می افتند. وقتی چیزی ممکن باشد که از عمل بایستد بالاخره این اتفاق خواهد افتاد بهتر است آینده نگر باشیم.

موفق و پیروز باشید

بهمن ماه ۱۳۹۴

مهدی رجبی